NIST Special Publication 1232

NIST Conference Papers Fiscal Year 2016

Compiled and edited by:

Andrea Medina-Smith
Kathryn Miller
Karen Wick

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1232

NIST Conference Papers
Fiscal Year 2016

Compiled and edited by:

Andrea Medina-Smith
Kathryn Miller
Karen Wick
Information Services Office

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1232

October 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1232
Natl. Inst. Stand. Technol. Spec. Publ. 1232, 1118 pages (October 2018)
CODEN: NSPUE2

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1232

Foreword

NIST is committed to the idea that results of federally funded research are a valuable national resource and a strategic asset. To the extent feasible and consistent with law, agency mission, resource constraints, and U.S. national, homeland, and economic security, NIST will promote the deposit of scientific data arising from unclassified research and programs, funded wholly or in part by NIST, except for Standard Reference Data, free of charge in publicly accessible databases. Subject to the same conditions and constraints listed above, NIST also intends to make freely available to the public, in publicly accessible repositories, all peer-reviewed scholarly publications arising from unclassified research and programs funded wholly or in part by NIST.

This Special Publication represents the work of NIST researchers at professional conferences in Fiscal Year 2016.

More information on public access to NIST research is available at https://www.nist.gov/open.

Table of Contents

Oliver; Ma, Lijun; Tang, Xiao. "Characterization of type-II spontaneous parametric down-conversion in domain-engineered PPLN." Paper presented at SPIE OPTO, San Francisco, CA, Feb 13-Feb 18, 2016. . . . . SP-468

Lechevalier, David; Shin, Seungjun; Woo, Jungyub; Rachuri, Sudarsan; Foufou, Sebti. "A virtual milling machine model to generate machine-itoring data for predictive analytics." Paper presented at the The Product Lifecycle Management (PLM) Conference 2015, Doha, Qatar, Oct 19-Oct 21, 2015. . . . . SP-477

Lechevalier, David; Narayanan, Anantha Narayanan; Rachuri, Sudarsan; Foufou, Sebti; Lee, Yung-T. "Model-based engineering for the integration of manufacturing system with advanced analytics." Paper presented at the 13th IFIP International Conference on Product Lifecycle Management (PLM16), Columbia, SC, Jul 11-Jul 13, 2016. . . . . SP-487

Lee, Vincent; Phillips, Steven; Shakarji, Craig; Hosto, Jeffrey; Huber, Jeffrey; Barbara, Gillich. "Design and calibration of an artifact for evaluating laser scanning articulating arm CMMs used for measuring complex non-concurrent surfaces." Paper presented at the 30th ASPE Annual Meeting: Precision Metrology, Austin, TX, Oct 31-Nov 5, 2015.. . . . . SP-498

Levine, Zachary; Genc, Karim; Luke, Stephen; Pietiela, Todd; Cotton, Ross; Ache, Benjamin; Young, Phillipe; Horner, Marc; Townsand, Kevin. " Towards Estimating the Uncertainty Associated with 3D Geometry Reconstructions From Medical Image Data." Paper presented at the 2016 BMES/FDA Frontiers in Medical Devices Conference, College Park, MD, May 25-May 27, 2016. . . . . SP-503

Li, Yunpeng; Roy, Utpal; Shin, Seungjun; Lee, Yung-T. "A 'Smart Component' Data Model in PLM." Paper presented at the 2015 IEEE International Conference on Big Data, Santa Clara, CA, Oct 29-Nov 1, 2015. . . . . SP-504

Linteris, Gregory; Takahashi, Fumiaki; Katta, Viswanath; Babushok, Valeri. "Extinguishment and Enhancement of Propane Cup-Burner Flames by Halon and Alternative Agents." Paper presented at the Eighth

Purdy, Thomas; Grutter, Karen; Srinivasan, Kartik; Klimov, Nikolai; Ahmed, Zeeshan; Taylor, Jacob. "Thermometry with Optomechanical Cavities." Paper presented at the OSA Conference on Lasers and Electro-optics (CLEO), San Jose, CA, Jun 5-Jun 10, 2016. . . . . SP-788

Putorti Jr., Anthony; Melly, Nicholas; Bareham, Scott; Praydis, Joseph. " Characterizing the thermal effects of High Energy Arc Faults." Paper presented at SMiRT 23 - 14th International Seminar on Fire Safety in Nuclear Power Plants and Installations (GRS-A-3845), Salford, United Kingdom, Aug 17-Aug 18, 2015. . . . . SP-790

Rachakonda, Prem; Muralikrishnan, Balasubramanian; Shakarji, Craig; Lee, Vincent; Sawyer, Daniel. "Evaluation of the Range Performance of Laser Scanners Using Non-Planar Targets." Paper presented at the 30th ASPE Annual meeting, Austin, TX, Nov 1-Nov 6, 2015. . . . . SP-803

Rachakonda, Prem; Muralikrishnan, Balasubramanian; Shilling, Katharine; Cheok, Geraldine; Lee, Vincent; Blackburn, Christopher; Everett, Dennis; Sawyer, Daniel. "Targets for Relative Range Error Measurement of 3D Imaging Systems." Paper presented at The Coordinate Metrology Society Conference, Nashville, TN, Jul 25-Jul 29, 2016. . . . . SP-809

Ren, Wei; Sundahl, Roy; Doiron, Theodore. "On The Feasibility of Performing Line Scale Measurements on a High Accuracy Coordinate Measuring Machine." Paper presented at the NCSLI 2016 Workshop & Symposium Exhibition, Saint Paul, MN, Jul 24-Jul 28, 2016.. . . . . SP-821

Rhee, Sokwoo. "Catalyzing the Internet of Things and Smart Cities: Global City Teams Challenge." Paper presented at the First International Workshop on Science of Smart City Operations and Platforms, Vienna, Austria, Apr 11-Apr 11, 2016. . . . . SP-829

Rouil, Richard; Cintron, Fernando; Ben Mosbah, Aziza; Gamboa Quintiliani, Samantha. "An LTE Device-to-Device module for ns-3." Paper presented at the WNS3, Seattle, WA, Jun 15-Jun 16, 2016. . . . . SP-833

Ruemler, Shawn; Zimmerman, Kyle; Hartman, Nathan; Hedberg, Thomas;

WafterBond ’15 – Conference on Wafer Bonding for Microsystems, 3D- and Wafer Level Integration

A ROUND ROBIN EXPERIMENT TO SUPPORT BOND VOID MEASUREMENT STANDARDS

Richard A. Allen[1], David T. Read[1], Victor H. Vartanian[2], Winthrop A. Baylies[3], William Kerr[4], Mark Plemmons[4], Noel Poduje[4], and Kevin Turner[5]
[1]National Institute of Standards and Technology, [2]SEMATECH, [3]Baytech-Resor, [4]Evergreen Enhancement, and [5]University of Pennsylvania

Abstract

A round robin experiment to compare the sensitivities of various metrology tools to small voids between bonded wafers such as are used in three-dimensional stacked integrated circuits (3DS-ICs) and MEMS packaging. Participants received a set of four bonded wafer pairs with programmed voids from 0.5 µm to 300 µm in the bond plane; each wafer pair had different void depth ranging from 40 nm to 1200 nm. This experiment highlighted the capabilities and limits of various infrared (IR) and acoustic microscopies, including factors such as speed of measurement and resolution.

Introduction

To support the growing application of wafer bonding to three-dimensional stacked integrated circuits (3DS-ICs) and MEMS devices, the SEMI 3OS-IC Committee initialed a round robin experiment to compare the sensitivities of various metrology tools to small voids between wafers. Bond voids have been a long-standing concern in MEMS packaging, which rely on bonding to provide a hermetic seal isolating mechanical devices from the environment, and are a major roadblock to the implementation of direct wafer bonding for 3DS-ICs.

Random inhomogeneities, such as particles, trapped gasses, or non-uniformities in the surface layer, are typical sources of bond voids. The diameter and depth of any particular void is highly dependent on small variations in the inhomogeneity. Thus, this experiment used test wafers with programmed voids.

Also, the original goal of this experiment was a standard **Test Method** for measuring voids[1]. As the project advanced it became clear that the individual capabilities of the variety of metrology tools available were complementary and it made sense to develop the initial standard as a **Guide** document [2].

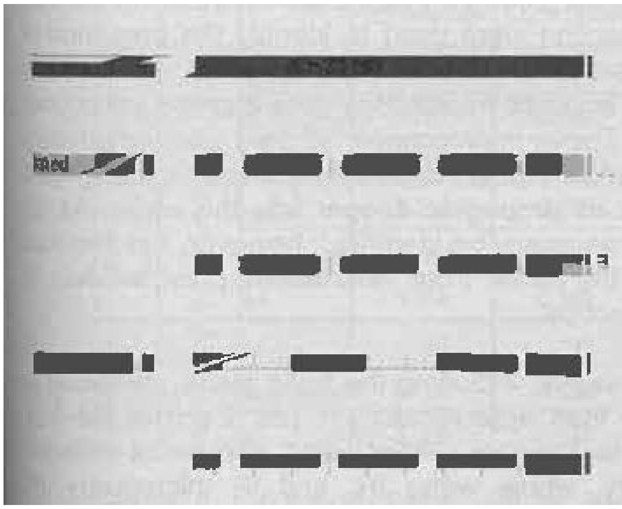


Figure 1. Layout of a *single test chip*

Allen, Richard; Read, David; Vartanian, Victor; Baylies, Winthrop; Kerr, William; Plems, Mark; Turner, Kevin.
“A Round Robin Experiment to Support Bond Void Measurement Standards.”
Paper presented at the Conference on Wafer Bonding for Microsystems 3S- and Wafer Level Integration, Braunschweig, Germany, Dec 8-Dec 9, 2015.

Test Wafer Design and Fabrication

A 25 mm by 32 mm test chip, incorporating a set of 18 test structures, was developed for this experiment (Figure 1). The individual test structures consist of an array of patterned voids, arranged so that there are isolated (» 5:1 space to width), semidense (5:1), and dense (1:1) voids. The design dimensions of these voids range from 0.5 µm to 300 µm.

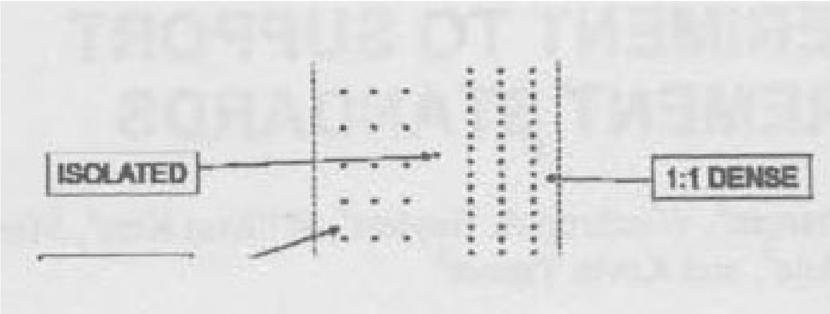


Figure 2. Isolated, semi-dense, and dense programmed voids within a block in the test chip

A thermal oxide, nominally 5 nm thick was grown on approximately 25 sets of four pairs of 300 mm silicon wafers. Photoresist was deposited onto one wafer from each pairs and the test chip was imaged on 51 sites on each wafer. The pattern was transferred into the oxide and the photoresist was then removed. One pair of wafers (one patterned, one unpatterned) was set aside. The pattern on the remaining three patterned wafers was then etched into the underlying silicon, using the oxide as a hard mask. The additional etch on the three wafers was 400 nm, 900 nm, and 1200 nm, respectively. After etching, each patterned wafer was bonded to an unpattemed cap wafer using an oxide bond process. A cross-section of the process is shown in Figure 3

Round Robin Experiment

A number of laboratories involved in MEMS and 3DS-IC packaging research and production volunteered to participate in the experiment. These laboratories included device manufacturers, metrology tool suppliers, and academic. The experiment was described to the laboratories and they were asked to measure these devices using experiment broadly fell into three
categories: those using ultrasonic inspection to identify and/or characterize voids, those that use infrared light, and those that use x-rays. Reports were returned from ten laboratories, with two reporting null results and the other eight providing data from one or more of the wafers [3].

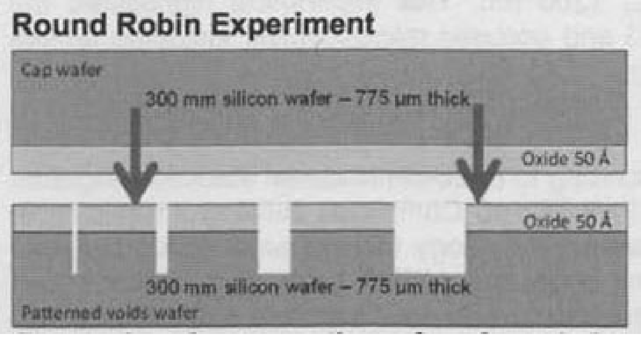


Figure 3. Cross section of wafers bond process

Ultrasonic techniques in this experiment included full-wafer resonance at frequencies around 40 kHz. This technique involves inducing vibrations in the bonded wafer pair and monitoring the response signal.

Differences in the frequency response between a void-free bonded pair and the bonded pair under inspection were used to identify the presence of void. This technique provides a fast, qualitative indication of bond voids. One of the laboratories utilized this technology. Scanning acoustic microscopy uses a single transducer as source and to measure the return signal. These microscopes typically use transducers with resonant frequencies between 5 MHz and 500 MHz. Higher frequencies typically give better spatial resolution while lower frequencies propagate deeper into the wafer. As air gaps reflect 100% of the signal, bond voids can easily be identified; however, this requires a coupling fluid between the transducer and the wafer. Four laboratories provided data to the experiment using scanning acoustic microscopy.

Infrared light is used to image the interior of wafers, including the bond plane, as silicon is transparent to light with wavelengths longer than approximately 1 µm. Each of the four laboratories contributing tR measurements to the experiment used somewhat different technologies including infrared interferometry, whole wafer IR, and IR microscopy. IR microscopy perhaps gives the most detailed images of voids [4]; however, the time to capture images using IR microscopy make it best used for characterizing voids identified using other techniques. The final IR tool was the grey-field polariscope. This technique captures the polarization of IR light transmitted through a bond wafer pair, which in turn is a function of stress in the wafer. This tool showed a limitation of the artificial voids used in this experiment: while voids *in situ are* caused by processes that invariably introduce stress around the void, this metrology was not sensitive to the artificial voids, which do not induce stress in the wafers.

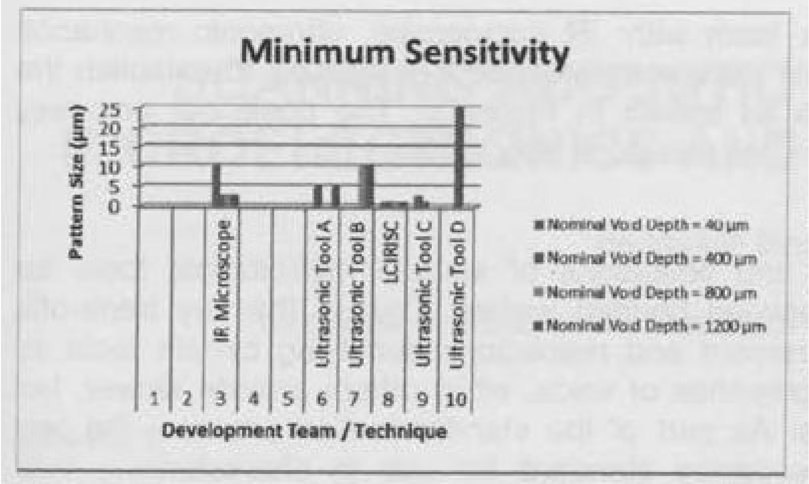
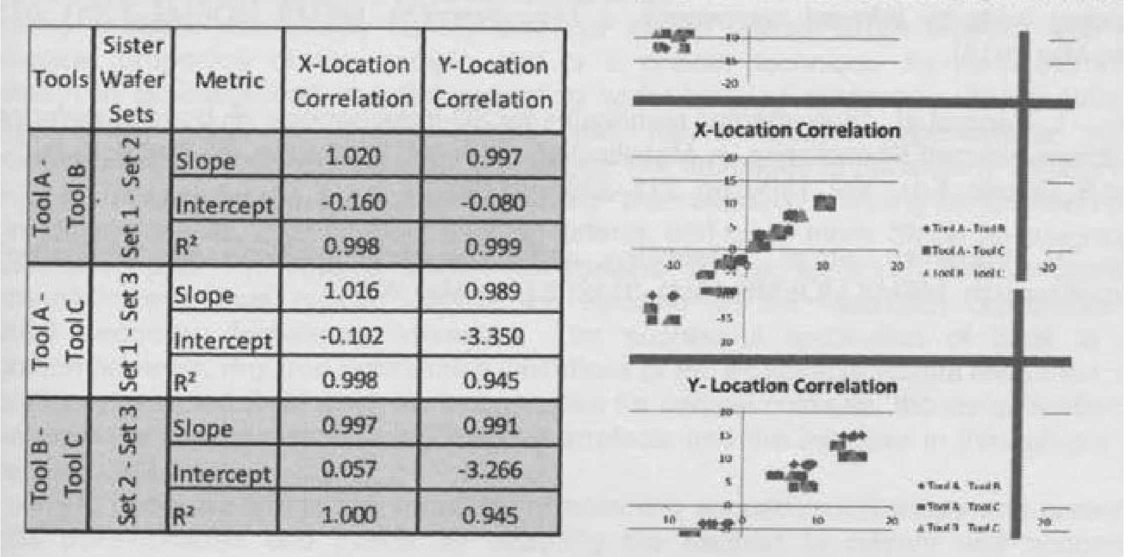


Figure 4. Minimum sensitivities for three measurement methods.

The metrology tool used by the final laboratory was X-ray tomography. This technique has been shown to be useful for imaging various buried features in 3D stacked integrated circuits [5], [6]; however, since these samples, composed only of silicon and SiO_2, were transparent to x-rays, yielding no usable data.

Experimental Results: Defect Detection

Three systems will be considered for defect detection and location correlation: ultrasonic resonance spectroscope, infrared microscope, and Low Coherence InfraRed Interferometry scanning (LCIRISC) system. The measurement techniques employed yield different results based on film thickness and measurement technique. Figure 4 shows the minimum sensitivities range from 1 µm to 25 µm for all of the teams that reported results. The LCIRISC system shows a consistent 1 µm minimum sensitivity for all void depths. Ultrasonic Tool C also shows a 1 µm minimum sensitivity for 400 µm void depth. The other systems had greater than 1 µm minimum sensitivity on all void depths.



Tools	Sister Wafer Sets	Metric	X-Location Correlation	Y-Location Correlation
Tool A - Tool B	Set 1 - Set 2	Slope	1.020	0.997
		Intercept	-0.160	-0.080
		R²	0.998	0.999
Tool A - Tool C	Set 1 - Set 3	Slope	1.016	0.989
		Intercept	-0.102	-3.350
		R²	0.998	0.945
Tool B - Tool C	Set 2 - Set 3	Slope	0.997	0.991
		Intercept	0.057	-3.266
		R²	1.000	0.945

X-Location Correlation
20
15
10
5
-10
10
20
-15
-20
Tool A - Tool B
Tool A - Tool C
Tool B - Tool C
Y- Location Correlation
20
15
10
5
0
10
20
Tool A - Tool B
Tool A - Tool C
Tool B - Tool C

Figure 5. X-Y correlation results, where Tool A = LCIRISC, Tool B = IR microscope, Tool C = Acoustic microscope. All units in micrometers.

Experimental Results: Location Correlation

Three sets of sister wafers were established for the purpose of location correlation. One set of sister wafers was provided to each team with: IR microscope, ultrasonic resonance spectroscope, and LCIRICS. These tools were correlated for X-Y location to establish the positional consistency across platforms as shown in Figure 5. The positional accuracy across systems correlates well with R2 > 0.99 and slope approaching 1.0.

Conclusions and Future Work

These results highlight the strengths and limitations of several metrological tools for identifying and characterizing voids between bonded wafers. One of the key trade-offs observed is between speed of measurement and resolution, identifying certain tools as being better for quickly identifying the presence of voids, while others provide slower, but more detailed characterization of voids. As part of the standardization process, the test structure is being developed into a separate standard for use in characterizing void metrology tools. Several laboratories were unable to complete their measurements in time for inclusion in the first version of SEMI 3013; as data from these laboratories becomes available it will be incorporated into the document. Finally, as these different metrologies and processes become more mature, it is likely that one or more will be adopted into standalone **Test Method** documents.

Acknowledgements

The authors would like to thank ...

References

(1) R. A. Allen, et al., lntercomparison of Methods for Detecting and Characterizing Voids in Bonded Wafer Pairs, ECS Transactions, 33 (4) 581-.589 (2010).

[2] 3D13-0715, Guide for Measuring Voids in Bonded Wafer Stacks, SEMI, San Jose, California, U.S.A. Available from www.semi.org.

[3] AUX-032-0715, Round Robin Study of Method for Measurement of Voids in Bonded Pairs of Silicon Wafers, SEMI, San Jose, California, U.S.A. Available from www.semi.org.
[4] J. Höglund, et al., Detection and characterization of three-dimensional interconnect bonding voids by infrared microscopy, J. Micro/Nanolith. MEMS MOEMS 13(1), 011208 (Jan-Mar 2014).
[5] L. Kong et al., "Sub-imaging techniques for 3O-interconnects on bonded wafer pairs,” in Stress-Induced Phenomena, in Metallization: 11th Int. Workshop, E. Zschech, P. S. Ho, and S. Ogawa, Eds., Vol. 1300, pp. 221-228, AIP (2010).
[6] V. Vartanian, et al., "Metrology needs for through-silicon via fabrication”, J. Micro/Nanolith. MEMS MOEMS 13(1), 011206 (Jan-Mar 2014).

A set-theoretic approach to analyzing timing uncertainty within cyber-physical systems

D.M. Anand, *National Institute of Standards and Technology*
Gaithersburg, MD 20899

BIOGRAPHY (IES)

D. M. Anand is a Research Scientist with the National Institute of Standards and Technology. His research interests include the dynamics, control, fault diagnosis and optimization of distributed networked systems. Application domains of particular interest include power systems, industrial control systems and cyber-physical systems where humans participate cognitively.

ABSTRACT

Clocks are deeply integrated into practically every cyber-physical system either explicitly as provenance for time-triggered actions, or implicitly in cases where cyber components operate in lock step with physical dynamics. Recognizing the criticality of timing components, this paper investigates an analysis approach that allows a system designer to formally incorporate timing uncertainty as a factor when evaluating the uncertainty of the overall cyber-physical system. A set theoretic approach is considered in this paper that offers advantages in the form of computational scalability and in its ability to accommodate a general class of hybrid dynamic systems. A demonstration of the approach is provided via illustrative example using a charge pump phase locked loop and a second order dynamic system. We anticipate that the proposed approach is particularly applicable to systems where safety or reachability guarantees are required.

1) INTRODUCTION

Unification and global traceability of time scales are particularly critical in systems spread over a wide geographical area where collaborative actions between components are frequently imputed to UTC. Examples of such systems include the cellular telecom network, the electric power system and wide area process control systems (pipelines and gas supply networks).

Most of these cyber-physical systems (CPS) involve controllers, consisting of: (a) a set of sensors and actuators, representing the interface between the controller and its environment; (b) a control logic (implemented as one or more circuits or as one or more pieces of software running concurrently); and (c) the underlying timing system, which determines the rate, precision and accuracy of coordinated actions. Such systems are commonly modeled as hybrid automata. Hybrid automata are finite-state machines equipped with continuous variables. Each discrete state of an automaton has a system of differential equations that govern its continuous variables.

When designing a CPS or while integrating components into a CPS, designers typically perform correctness tests of the system as a whole. These tests typically evaluate all likely behaviors or trajectories of the system against a set of 'performance' criteria [1]. A simplified notion of performance would be that the system provides the minimum expected functionality while not entering an unsafe or bad state. Ensuring correctness, however, is often not a trivial task. Simulation of the system is not adequate, since it can only help examine a limited number of trajectories. Analytical methods are often not applicable, considering the complexity of systems with a large number of dynamic interactions.

Analytical and simulation studies are particularly inadequate when assessing the safety of a closed-loop CPS in relation to uncertainty associated with timing components [2]. Firstly, the timing system is a CPS in itself, characterized by interacting continuous (Phase and Frequency Locking) and discrete (Synchronization logic) states. Further, the stochastic properties of oscillators are rarely amenable to closed form analytical expression. And lastly, manufacturer data for clocks frequently represent uncertainty in the form of bounded sets (min/max, PPM) making simulation studies impractical.

An alternative to analytical and simulation studies is reachability analysis [3]. It consists of computing the set of all reachable states of the system and then checking that an application specific safe set encloses it. In our paper we focus on analyzing the impact of timing uncertainty on safety criteria. Reachability, as used in our analysis, involves mapping the performance envelope for the timing system onto the safe set for an enclosing CPS.

In our paper we consider a timing subsystem comprised of a Type-II Charge Pump Phase Locked Loop (PLL) and model (as hybrid automata) the interactions between a VCO, a three state phase frequency detector, a loop filter and frequency divider.

In Section 2 we present the model of our system including the hybrid automata we use to describe it. In Sections 3 and 4 we introduce our geometric interpretation of

Anand, Dhananjay; Arafin, Tanvir; Qu, Gang.
"Detecting GNSS Spoofing using a Network of Hardware Oscillators."
Paper presented at the Annual Precise Time and Time Interval (PTTI) Systems and Applications Meeting, Monterey, CA, Jan 25-Jan 28, 2016.

uncertainty and apply it to sensor uncertainty and uncertainties associated with the PLL system respectively. Section 5 presents hybrid set theoretic reachability and the geometric results that enable our analysis. Finally, Section 6 concludes our analysis by highlighting some preliminary results showing that the correctness of a synchronous generator control system can be evaluated from the perspective of measurement uncertainty (combining sensor and timing uncertainty) using our set theoretic approach. We also propose next steps for the work presented in this paper.

2) HYBRID AUTOMATA

A linear hybrid automaton is a generalized finite state automaton that is equipped with continuous variables. The discrete changes of the hybrid system are modeled by edges of the automaton and the continuous evolution of the system at each location in the automaton is constrained by linear time invariant dynamics of the form $\dot{x} = Ax + Bu$. The syntax we use for hybrid automaton in our paper is defined in detail in [4].

Following conventional notation, let us consider a hybrid automaton H represented by the tuple $\langle Loc, Edge, \Sigma, X, Init, Flow, Jump \rangle$ where Loc: $\{l_1, l_2 \dots l_m\}$ is a set of finite control locations that represent control modes. Instantaneous discrete transitions between control modes are denoted with a set of labeled edges $Edge \subseteq \Sigma \times Loc$ where the labels are drawn from set Σ. The automaton is equipped with a set of differentiable continuous variables $X \in \mathbb{R}^n$, with $\dot{X}$ and $\acute{X}$ representing the first derivative and the updated value of X respectively. The $Init$ and Inv predicates attached to each location in the automaton represent inequality constraints on the initial value and magnitude limits of X within each mode respectively. Finally, the functions $Flow$ and $Jump$ represent the evolution trajectory acting on $X \cup \dot{X}$ and the discrete update acting on $X \cup \acute{X}$ respectively.

2.1) Running CPS example

To illustrate the analysis approach in this paper let us consider a simplified example of a control problem requiring synchronized clocks. The example we use in this paper is based on the control requirements for power regulation in a 'microgrid' [5]. Microgrids with multiple generators require precise coordination of generator set points in order to maintain stable voltage and frequency. This coordination is particularly critical in a small power grid that is susceptible to fluctuations in voltage magnitude and frequency due to changes in loads, or external conditions such as a fault on the main grid. Control methodologies must respond to local variations in voltage waveforms, while still tracking a reference performance schedule for the microgrid. Since microgrids can span several hundred meters in area, control and sensor signals are typically transmitted over an Ethernet network, with control authority delegated to multiple generators. Accurate clock synchronization is required across all generators, sensors and circuit breakers to ensure operation of the entire networked control system.

A simplified dynamic representation of the microgrid problem is shown in Figure 1. In our example, we assume two generators represented by the linearized swing dynamics as shown in Equation 1 coupled through a complex impedance Z_{12}. This simplified example highlights the coupling interaction between two sets of 2nd order differential equations. In the case of our example, the impedance between the generators manifests dynamics corresponding to a first order filter in the form of a phase lag between b_1 and b_2. The dynamic response of each generator is governed by its rotary inertia and damping ratio J_i and D_i respectively. The state of each generator is represented by its terminal voltage E_i and rotor angle δ_i. The generator is controlled via regulation of input power $P_{g,i}$. The cumulative dynamics of the two-generator system in response to perturbations of the state $[V_i, \theta_i]^T$ about a synchronized network in steady state may be represented by the dynamic linearized swing equation and the algebraic DC power flow equation. These equations can be assembled into a state-space model for the network, producing a small signal version of the structure-preserving power network model shown in Equation 2 as derived in [6].

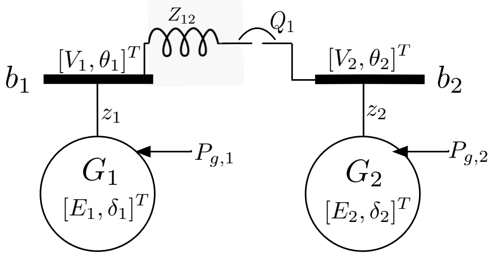


Figure 1: Schematic representation of a two generator microgrid

Equation 1: Linearized swing equation for generators

$$\dot{\delta}_i(t) = \omega_i(t),$$
$$J_i\dot{\omega}_i = P_{g,i}(t) - \frac{E_iV_i}{z_i}(\delta_i(t) - \theta_i(t)) - D_i\omega_i(t)$$

Equation 2: Structure preserving power network model

$$\begin{bmatrix} I & 0 & 0 \\ 0 & J & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta}(t) \\ \dot{\omega}(t) \\ \dot{\theta}(t) \end{bmatrix} = - \begin{bmatrix} 0 & -I & 0 \\ L_{gg} & D & L_{gl} \\ L_{lg} & 0 & L_{ll} \end{bmatrix} \begin{bmatrix} \delta(t) \\ \omega(t) \\ \theta(t) \end{bmatrix} + \begin{bmatrix} 0_{(1:n)} \\ Pg_{(1:n)} \\ P_{(1:m)} \end{bmatrix}$$

Assuming that the generators in the network are of PV-Type [7], we can decouple Equation 2 into a system of Ordinary Differential Equations in the linear time invariant form $\dot{x} = Ax + Bu$ and a set of linear algebraic constraints $\alpha \geq [\mathbb{Z}_{12}]^{-1}\, x$ on the relative phase between adjacent buses where $[\mathbb{Z}_{12}]$ is the impedance weighted adjacency matrix for the two generator circuit. Note that such algebraic constraints are compatible with the Inv

predicate defined in Section 2. Let us now consider the discrete changes in the circuit topology represented by the circuit breaker Q_1. In the event of a large fault current between b_1 and b_2, the phase constraint represented by Z_{12} is released and the two generators operate independently. In power systems terms, this event represents a fault triggered decoupling event. Q_1 may be triggered by other considerations such as a phase angle, thermal or voltage excursions. In our formalism for hybrid automata these triggers comprise the $Jump$ predicate.

Without the loss of generality, we can reduce the microgrid regulation control problem within each operating mode of the circuit breaker to a phase synchronization problem for G_2. The synchronization torque for G_2 is given by the equation:

$$P_{g,2} = \frac{V_1 V_2}{Z_{12}} \cos(\theta_1 - \theta_2)$$

Integrating this control law into the dynamics in Equation 2 and linearizing the system we get a closed loop system of the form $\dot{x} = [A + BK]x$. The closed loop system after a circuit breaker tripping event is represented by $\dot{x} = [A^* + BK^*]x$. Combining both operating modes, we get the hybrid system shown in Figure 2.

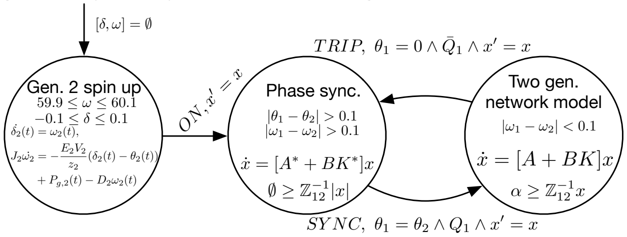

$[\delta, \omega] = \emptyset$
Gen. 2 spin up
$59.9 \leq \omega \leq 60.1$
$-0.1 \leq \delta \leq 0.1$
$\dot{\delta_2}(t) = \omega_2(t),$
$J_2\dot{\omega_2} = -\frac{E_2V_2}{z_2}(\delta_2(t) - \theta_2(t))$
$+ P_{g,2}(t) - D_2\omega_2(t)$
$ON, x' = x$
Phase sync.
$|\theta_1 - \theta_2| > 0.1$
$|\omega_1 - \omega_2| > 0.1$
$\dot{x} = [A^* + BK^*]x$
$\emptyset \geq \mathbb{Z}_{12}^{-1}|x|$
$TRIP,\ \theta_1 = 0 \wedge \bar{Q}_1 \wedge x' = x$
Two gen. network model
$|\omega_1 - \omega_2| < 0.1$
$\dot{x} = [A + BK]x$
$\alpha \geq \mathbb{Z}_{12}^{-1}x$
$SYNC,\ \theta_1 = \theta_2 \wedge Q_1 \wedge x' = x$

Figure 2: Hybrid automata describing the three operating modes for the two generator system.

3) SENSOR UNCERTAINTY

The sources of uncertainty that limit the performance of the phase tracking control problem range from model errors, to inaccuracies in measurements to actuator bandwidth limitations and network latency. Since Equation 1 has an inherent pole at the origin (an integrator), our generator phase synchronization problem presents a tracking error that is proportional to the integral of any error in the control inputs. The control input $P_{g,i}$ in turn, is an algebraic function of the system state with a gain proportional to Z_{12}^{-1}. For most distribution circuits, this gain is in the order of about 10^4 making the control system particularly sensitive to uncertainties in the system state x.

Inaccuracies in the estimation/measurement of the system state will be the primary focus of our analysis in this paper in keeping with growing interest in the microgrid community for real time, high quality sensor measurements. The state of our example system (Equation 2) includes the explicit variables $[\theta, \delta]$ that correspond to measurements of phase on circuit buses and generator terminals respectively. These measurements are typically obtained using a Phasor Measurement Unit (PMU). PMUs estimate the phase, frequency, frequency modulation and amplitude of the fundamental grid frequency (60Hz in the U.S.). The primary PMU generated measurement, however, is called a synchrophasor which is a vector representation of a sinusoidal voltage and current waveform as illustrated in Figure 3.

Several algorithms exist to compute the synchrophasor, however a majority of the algorithms utilize a recursive peak tracking implementation of the discrete Fourier transform or a similar algorithm [8]. The synchrophasor phase angle θ is measured in reference to the 'second' transition on a UTC synchronized clock within the PMU. As a result, clock offsets in the PMU clock manifest as phase error of the vector measurement [9].

The C37.118.1-2011 synchrophasor standard and its amendment [10], [11] bound the total vector error (TVE) for synchrophasors to a threshold ϵ (typically $\epsilon \leq 1\%$ under steady state conditions). TVE is the magnitude of the error vector between the true synchrophasor for a given sinusoidal waveform to the phasor measured by the PMU. The TVE bound includes all sources of error within the PMU including errors in the potential transformers and other transducers, limitations in sampling, A/D conversion and timing errors. The TVE limit is illustrated in Figure 3 by a circle with radius ϵ. Note that the maximum tolerable phase error PE is represented by tangents to the circular TVE region.

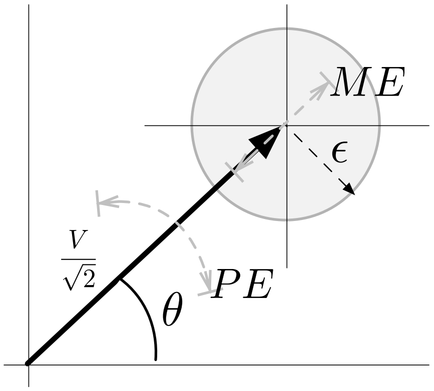


Figure 3: A synchrophasor plotted on the I/Q plane showing limits for total vector error.

Equation 3: TVE in terms of magnitude and phase error

$$TVE^2(\%) = \left\{ \left[\left(1 + \frac{ME(\%)}{100} \right) \cos(PE) - 1 \right]^2 + \left[\left(1 + \frac{ME(\%)}{100} \right) \sin(PE) \right]^2 \right\} \times 100\%$$

Transforming the TVE criterion from the I/Q plane to a real basis of magnitude and phase errors, we get the relation shown in Equation 3. Where PE and ME correspond to phase and percent magnitude errors respectively. An interesting outcome of this change of basis is that the graphical interpretation of Equation 3 is an ellipsoidal level set.

Figure 4 shows the level curves for Equation 3 at different values of ϵ. Based on this geometric interpretation, we propose that uncertainty in the system state x for the microgrid system, as measured by a PMU, may be represented by a spherical or hyper-ellipsoidal geometric error criterion. Our uncertainty model is not stochastic but rather deterministic and set based. In the following sections, we will extend this interpretation of uncertainty and generalize our uncertainty model in order to develop a non-probabilistic test for safety or correctness of the two generator power system for any realization of state uncertainty within the set.

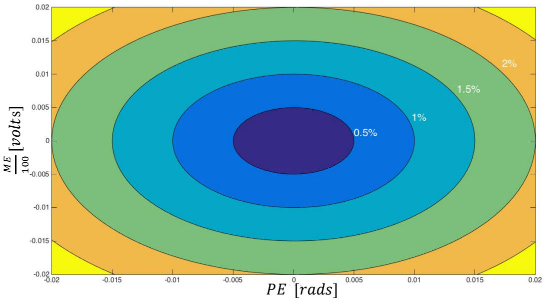


Figure 4: Contour plot showing ellipsoidal level curves corresponding to different values of ϵ

4) UNCERTAINTY FROM TIMING COMPONENTS

An important factor affecting PMU performance is its internal timing system. As highlighted in the previous section, timing errors result in errors in measurement of phase. Prior evaluations of PMU performance and uncertainty include timing errors in their analysis by simply translating the maximum tolerable measurement error to the corresponding clock offset i.e. for the $\epsilon \leq 1\%$ criterion to hold in a 60 Hz system, errors in the timing system must be ≤26.5 μs. Clearly, this is a fairly superficial treatment of timing errors. As the constraints on sensor performance are tightened and the complexity of algorithms used for CPS continually increase, there is concern in the metrology community that the dynamics associated with clock regulation and time synchronization might result in rare but unpredictable negative interactions within a CPS.

Let us re-examine PMU measurement uncertainty from the perspective of first order effects introduced by phase noise in the primary oscillator driving its sampling clock.

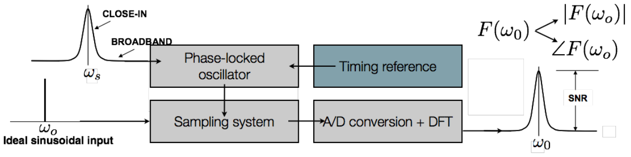


Figure 5: Schematic diagram showing measurement noise introduced through phase modulation of the sampling clock.

Assuming that the measurand is an ideal sinusoidal signal ω_0, Figure 5 illustrates the impact of phase noise in the sampling clock ω_s on the Signal-to-Noise ratio of the output signal $F(\omega_0)$ from the PMU [12]. When the sampling clock is derived from a free running oscillator its single side-band phase noise in dBc/Hz is typically a function of frequency offset from the oscillator resonant frequency. This function is available as published test data for the oscillator typically approximated to a number of regions having a slope of $^1/_{f^x}$. Figure 6 shows an example of this phase noise profile published in [13]. We assume for simplicity that the time domain jitter is dominated by "white" broadband phase noise. An assumption justified by the fact that sampling clocks in PMUs are typically phase locked oscillators. Phase locked loops significantly attenuate close-in phase noise. We can then compute the timing jitter introduced by the integrated noise power across a frequency domain of interest. Typically, a range of twice the sampling rate is adequate as shown in Figure 6 by the brown highlighted rectangular region.

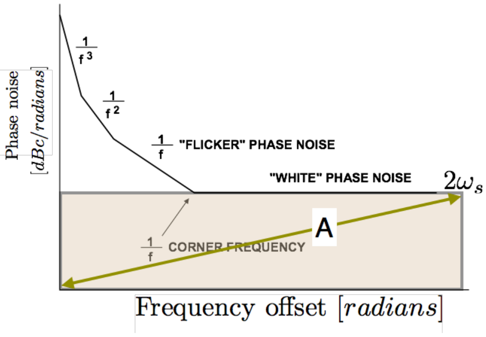


Figure 6: Oscillator phase noise profile

The root mean square timing jitter introduced by the total phase noise represented by the area labeled 'A' is given by:

$$T_{jitter} = \frac{\sqrt{2 \cdot 10^{A/10}}}{\omega_s}$$

We can now perform a change of basis in a similar fashion to the previous section to find the manifestation of this timing jitter in the output of an N-point Discrete Fourier Transform computed from discrete samples $f_n\ [n \in N]$.

First, assuming that T_{jitter} is uniformly distributed across the N sample DFT window, the standard deviation of the sampled signal in the time domain is given by:

$$U_n = \sqrt{\mathrm{E}[\alpha_n^2]} = \alpha_n \cdot T_{jitter}$$

Where α_n is the first derivative of the sampled sinusoidal (60Hz) waveform at sampling instant n.

Transforming this uncertainty to the phasor space or the I/Q plane as in Figure 3 we get the relation in Equation 4. See [14] for a more detailed presentation.

Equation 4: Uncertainty associated with sampling jitter

$$U^2_{I(\omega_0)}|T_{jitter} = \sum_{n=0}^{N-1} f_n \cos^2(\frac{\omega_0 n}{N}).U_n^2$$

$$U^2_{Q(\omega_0)}|T_{jitter} = \sum_{n=0}^{N-1} f_n \sin^2(\frac{\omega_0 n}{N}).U_n^2$$

$U^2_{I(\omega_0)}$ and $U^2_{Q(\omega_0)}$ correspond to the magnitude of uncertainty on the I and Q axes respectively. Adding these two terms we see that by the trigonometric identity $\sin^2 x + \cos^2 x = 1$ that the geometric interpretation of the cumulative uncertainty in signal magnitude and phase due to timing jitter is ellipsoidal in nature. As in Section 3 with sensor uncertainty, timing uncertainty can also be modeled using a set based hyper-ellipsoidal geometric error criterion.

4.1) Dynamics of timing components

Our analysis of timing uncertainty so far has focused on jitter and phase noise as ergodic parameters. There are also deterministic dynamics at play in the timing system that are seldom included when evaluating the correctness of CPS. For example, consider the dynamics of jitter mitigation and clock synchronization introduced into the sampling subsystem in a PMU. In the following analysis we focus on the dynamics of a three state charge-pump phase locked loop (3PD-CP-PLL) in conjunction with a voltage-controlled crystal oscillator (VCXO). This type of PLL is popular in embedded analog to digital converters and is unique in that the output of its phase detector is a current that is 'pumped' in and out of a loop-filter and is able to serve as a frequency detector as well. The reader is directed to [15]–[17] for more detailed discussion on PLL design illustrated in Figure 7.

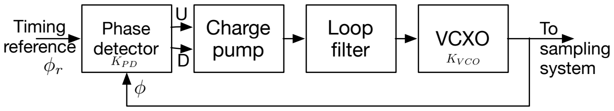


Figure 7: Block diagram of 3PD-CP-PLL driving the sampling system

The linearized closed loop dynamics associated with phase ϕ and frequency modulation ω due to the PLL can be described by the following differential equation:

$$\begin{bmatrix} \dot{\phi}(t) \\ \dot{\omega}(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -2K_{PD}K_{VCO}\cdot\omega_s & -2\omega_s \end{bmatrix} \begin{bmatrix} \phi(t) \\ \omega(t) \end{bmatrix} + \begin{bmatrix} 0 \\ 2K_{PD}K_{VCO}\cdot\omega_s \end{bmatrix}$$

The phase detector has three discrete operating modes (phase lead, phase lock and phase lag) that can be represented by the finite state machine in Figure 8. Note that the three state phase detector in conjunction with the linearized PLL dynamic equation produces a hybrid automata of the form described in Section 2.

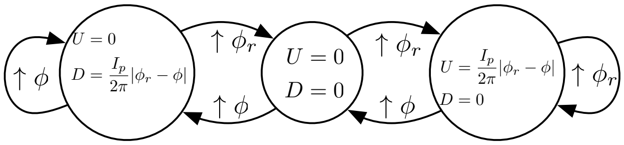


Figure 8: Hybrid system model of a three state phase detector.

The core challenge we address in our work is the propagation of uncertainty expressed in Equation 3 and Equation 4 through the dynamics shown in Figure 2 and Figure 8. In a larger sense, we are interested in a computationally feasible strategy to evaluate the impact of uncertainty originating from subsystems such as the timing system or the sampling system on the performance of a CPS. Our approach is a treatment of uncertainty using the same compositional primitives used to effectively compose a CPS from sub-systems. In the following section we will present one strategy to achieve this goal by exploiting the spherical and ellipsoidal fitting of geometric error criterion (such as TVE or Timing jitter) in $\mathbb{R}^n$.

5) REACHABILITY ANALYSIS

We treat uncertainty propagation as a dual to the problem of reachability of hybrid dynamic systems i.e., reach of a set of uncertain states represents a measure of correctness. In contrast to Monte-Carlo strategies of exploring the uncertainty space that are limited in scale to a finite number of simulated trajectories, we use a simplification of the uncertainty space represented as a convex set bounded by the functions in Equation 3 and Equation 4. Extending the observation that our convex uncertainty sets can be approximated by a family of hyper-ellipsoids $\mathcal{E}(q, Q) = \{x | \langle x - q, Q^{-1}(x - q)\rangle \leq 1\} [q \in \mathbb{R}^n, Q \in \mathbb{R}^{n\times n}]$ we use the results in [11] and [12] to propagate these ellipsoids through hybrid automata with small signal linear dynamics $\dot{x} \subseteq Ax + Bu$: Using the linear transformation $A[\mathcal{E}(q, Q)] + b = \mathcal{E}(Aq + b, AQA^T)$.

The guards of the discrete transition $X' \rightarrow X$ (recall the notation for the hybrid automaton H) are usually represented as linear inequalities. If the geometric interpretation of these inequalities is a half space $S = \{x | \langle b, x\rangle \geq \alpha\}$ then the ellipse $\mathcal{E}\big(q + (p), Q + (p)\big)$ is an approximation of $\mathcal{E}(q, Q) \cap S$ at any point $p \in \left[0, \frac{\alpha' + 1}{2}\right)$.
The geometric union of ellipsoids can also be estimated by an approximating ellipse $\mathcal{E}\big(q_1 + q_2, Q(\beta)\big) \subset \mathcal{E}(q_1, Q_1) \cup \mathcal{E}(q_2, Q_2)$ s.t. $Q(\beta) = (1 + \beta^{-1})Q_1 + (1 + \beta)Q_2 \ \forall\beta > 0$.

Using these geometric operations, we are able to analytically determine the correctness of hybrid systems for any realization of the uncertainty in a given set. As a result, correctness as evaluated using this approach is deterministic. In hybrid systems with a large number of interacting components, this deterministic approach consumes significantly less memory than comparable probabilistic approaches since each ellipse is stored as a tuple and every interaction between subsystems manifests as an intersection of ellipses which in turn is approximated as an ellipse. In comparison interacting dissimilar probability distributions result in very large sets of posterior probabilities.
Geometric operations for the intersection, union, linear transformation and geometric sum of convex sets can be performed very efficiently. As noted in [18], the complexity of the reachability analysis using ellipsoidal approximations is polynomial in time and quadratic in dimension. While a more detailed presentation of

verification guarantees for our ellipsoidal approximations are beyond the scope of this paper, we would like to highlight our approach as it applies to the CPS example in Section 2.1. First, the ability to efficiently detect intersections between ellipses and half spaces gives us a tool to test the hybrid system for violations such as the limit threshold on circuit breaker Q_1. Second, the geometric union of ellipses gives us the ability to compose multiple sources of uncertainty as in the uncertainty originating from PMUs expressed as TVE and the sampling jitter introduced by the timing system. Algorithms used to detect intersections and unions are either closed form, or guaranteed to converge to the global optimum in a finite number of iterations and they work without restriction in spaces of generic dimension. Lastly, the dynamics of the generators, the PLL system and the electrical network constraints are implemented as linear transformations on uncertainty ellipses. As described in [20], parameter uncertainty in dynamic models may also be expressed as unknown but bounded sets and so may be considered using our approach.

6) CONCLUSIONS AND FUTURE EXTENSIONS

As a preliminary evaluation of our approach, we considered two operating conditions for our CPS example. In the first case, an uncertainty set bounded by $\mathcal{E}\left\{\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}1 & 0\\0 & 0.5\end{bmatrix}\right\}$ was applied to the hybrid system comprising the charge pump PLL and the two generator network. Both systems are asymptotically stable in their primary operating modes and as a result $|Q|$ remains bounded as the reach set is propagated through the system dynamics. Figure 9 illustrates the evolution of reach set over ten simulated seconds constructing a 'reach tube'.

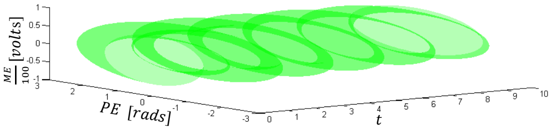


Figure 9: Reach tube showing stable evolution of phase and magnitude variation when the initial uncertainty set does not trip the circuit breaker.

Repeating the analysis for a case when the reach set intersects the half space facet representing a circuit breaker tripping event, we see that the same uncertainty set results in unbounded expansion of the reach set. Clearly not all trajectories are unstable within the set but the analysis does show that a sequence of dynamic transitions are possible that might drive the system to an unstable operating state. The phase tracking system, therefore, is no longer 'correct'.

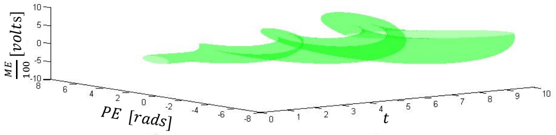


Figure 10: Reach tube showing an unstable evolution of phase and magnitude when the uncertainty set erroneously triggers a tripping event.

The analysis presented here is fairly simple in order to introduce our approach and to present its value to evaluating the correctness of hybrid dynamic systems; particularly in relation to the impact of timing uncertainty on large interconnected CPS. Our research continues to focus on this reachability approach for compositions of interconnected subsystems with a large number of set intersections. Our upcoming work includes simulations using real data for timing uncertainties and model parameters.

Official contribution of the National Institute of Standards and Technology; not subject to copyright in the United States. Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

REFERENCES

[1] R. Baheti and H. Gill, "Cyber-physical systems," *impact Control Technol.*, vol. 12, pp. 161–166, 2011.

[2] A. D. Stoyenko, *Constructing predictable real time systems*, vol. 146. Springer Science & Business Media, 2012.

[3] E. Asarin, O. Maler, and A. Pnueli, "Reachability analysis of dynamical systems having piecewise-constant derivatives," *Theor. Comput. Sci.*, vol. 138, no. 1, pp. 35–65, Feb. 1995.

[4] J.-F. Raskin, "An introduction to hybrid automata," in *Handbook of networked and embedded control systems*, Boston: Birkhäuser, 2005, pp. 491–517.

[5] M. Prodanovic and T. C. Green, "High-Quality Power Generation Through Distributed Control of a Power Park Microgrid," *IEEE Trans. Ind. Electron.*, 2006.

[6] F. Pasqualetti, A. Bicchi, and F. Bullo, "A graph-theoretical characterization of power network vulnerabilities," in *American Control Conference*, 2011.

[7] J. Glover, M. Sarma, and T. Overbye, *Power Systems Analysis and Design*. CL-Engineering, 2007.

[8] A. G. Phadke and B. Kasztenny, "Synchronized phasor and frequency measurement under transient conditions," *Power Deliv. IEEE Trans.*,

vol. 24, no. 1, pp. 89–95, 2009.

[9] K. Narendra, D. Gurusinghe, and A. Rajapakse, "Dynamic Performance Evaluation and Testing of Phasor Measurement Unit (PMU) as per IEEE C37. 118.1 Standard," *Int. Prot. Test. Users Gr.*

[10] P. S. R. Committee, "IEEE Standards for Synchrophasor Measurements for Power Systems-IEEE Std C37. 118.1-2011," New York, 2011.

[11] K. E. Martin, "Synchrophasor Measurements Under the IEEE Standard C37.118.1-2011 With Amendment C37.118.1a," *Power Deliv. IEEE Trans.*, vol. 30, no. 3, pp. 1514–1522, Jun. 2015.

[12] T. C. Weigandt, B. Kim, and P. R. Gray, "Analysis of timing jitter in CMOS ring oscillators," in *Circuits and Systems, 1994. ISCAS'94., 1994 IEEE International Symposium on*, 1994, vol. 4, pp. 27–30.

[13] W. Kester, "Converting Oscillator Phase Noise to Time Jitter," 2009.

[14] G. Betta, C. Liguori, and A. Pietrosanto, "Propagation of uncertainty in a discrete Fourier transform algorithm," *Measurement*, vol. 27, pp. 231–239, 2000.

[15] R. E. Best, *Phase locked loops*. McGraw-Hill Professional, 2007.

[16] C. A. Sharpe, "A 3-state phase detector can improve your next PLL design," *EDN Mag.*, vol. 9, pp. 55–59, 1976.

[17] M. Van Paemel, "Analysis of a charge-pump PLL: a new model," *IEEE Trans. Commun.*, vol. 42, no. 7, pp. 2490–2498, 1994.

[18] O. Botchkarev and S. Tripakis, "Verification of hybrid systems with linear differential inclusions using ellipsoidal approximations," *Hybrid Syst. Comput. Control*, pp. 73–88, 2000.

[19] R. Lorenz and S. Boyd, "An ellipsoidal approximation to the Hadamard product of ellipsoids," *IEEE Conference on Acoustics, Speech, and Signal Processing*. pp. 1193–1196, 2002.

[20] M. Milanese and A. Vicino, "Optimal estimation theory for dynamic systems with set membership uncertainty: an overview," in *Bounding Approaches to System Identification*, Springer, 1996, pp. 5–27.

OPTOMECHANICAL TRANSDUCER-BASED SOFT AND HIGH FREQUENCY NANOSCALE CANTILEVER FOR ATOMIC FORCE MICROSCOPY

S. An[1,2]*, J. Zou*[1,2]*, G. Holland*[1]*, J. Chae*[1,2]*, A. Centrone*[1]*, and V. Aksyuk*[1*]

[1] Center for Nanoscale Science and Technology, National Institute of Standard and Technology, Gaithersburg, Maryland, USA

[2]Maryland Nanocenter, University of Maryland, College Park, Maryland, USA

ABSTRACT

We introduce an optomechanical transducer-based nanoscale cantilever probe for atomic force microscopy (AFM). The high optical quality factor of the microdisk resonator enables detection of the nanoscale cantilever motion with high sensitivity. The low stiffness (≈ 1 N/m) and high frequency (above ≈ 4 MHz) nanoscale cantilever provides both a wide bandwidth for fast motion detection and a high force sensitivity. We demonstrate the capabilities of the device in AFM for fast scanning (nominal 30 μm × 30 μm, 39.06 Hz line rate, 2.93 mm/s tip speed) with a fast settling time (< 2 μs). Furthermore, the detection of photo-thermal induced resonance (PTIR) signals at a 50 nm thick polymer film is also demonstrated.

INTRODUCTION

Fast-scanning AFM with sensitive force measurement is essential for investigating short time-constant motion or dynamics at small scales, and the demand for this capability is growing rapidly in various fields of nanoscale science and technology [1-3]. The key to realizing the desired performance is the use of a cantilever with a high mechanical resonance frequency (ω), in order to provide a wide detection bandwidth, and a low stiffness (k), in order to provide high force sensitivity. These two goals can be realized by reducing the cantilever size to the nanoscale. However, if the cantilever size is reduced in this manner, optical transduction is inefficient for the typical beam bounce far-field or interferometric detection methods, used in conventional AFM systems. This occurs because the light cannot be focused only on the nanoscale cantilever due to the optical diffraction limit. For a given minimum size and mass (m), the stiffness increases with larger ω, since $k = m\omega^2$, resulting in low sensitivity.

Here we introduce a fully-integrated silicon microdisk cavity optomechanical transducer-based nanoscale cantilever to make a fast-scanning, sensitive AFM. An integrated near-field detection scheme [4] allows reduction of the mechanical probe cross-section to the 100 nm scale. A remarkable advantage of our cavity optomechanical transducer is its highly sensitive mechanical motion measurement, which is enabled by the strong interaction between photons that are confined inside the cavity and the cantilever motion. Optical shot noise, rather than thermal noise, fundamentally limits the motion readout precision, and optical power does not, in principle, have to be dissipated in the transducer. Readout precision is sufficient for the probe to operate at its fundamental thermo-mechanical limit. Among various types of optomechanical transducers such as suspended membranes [5], planar photonic crystal cavities [6], and microdisk resonators [7,8], we choose to utilize a microdisk type transducer for geometrical reasons: the cantilever can be simply incorporated around the rim of the microdisk, leading to an extended cantilever-disk interaction region, greatly enhancing the optomechanical coupling g_{OM}. This layout geometry facilitates the engineering of ω and k through geometry variations, and enables practical experiments in AFM systems. Furthermore, the integrated chip (optomechanical transducer and waveguide) is connected by optical fiber, which eliminates the need for laser alignment and provides a stable output signal.

We use a custom adapter to incorporate our transducer chip in place of a conventional AFM cantilever chip into a commercial AFM and PTIR system, and demonstrate improved performance of both instruments.

NANOFABRICATION OF THE DEVICE

Figure 1 shows the nanofabrication process of the device. The devices are fabricated in a 260 nm thick silicon layer on top of the 1 μm buried oxide (BOX) of a silicon-on-insulator (SOI) chip. Typically, multiple 5 mm × 5 mm individual die are fabricated on a single 3 cm × 3 cm chip. In this work electron (E)-beam and

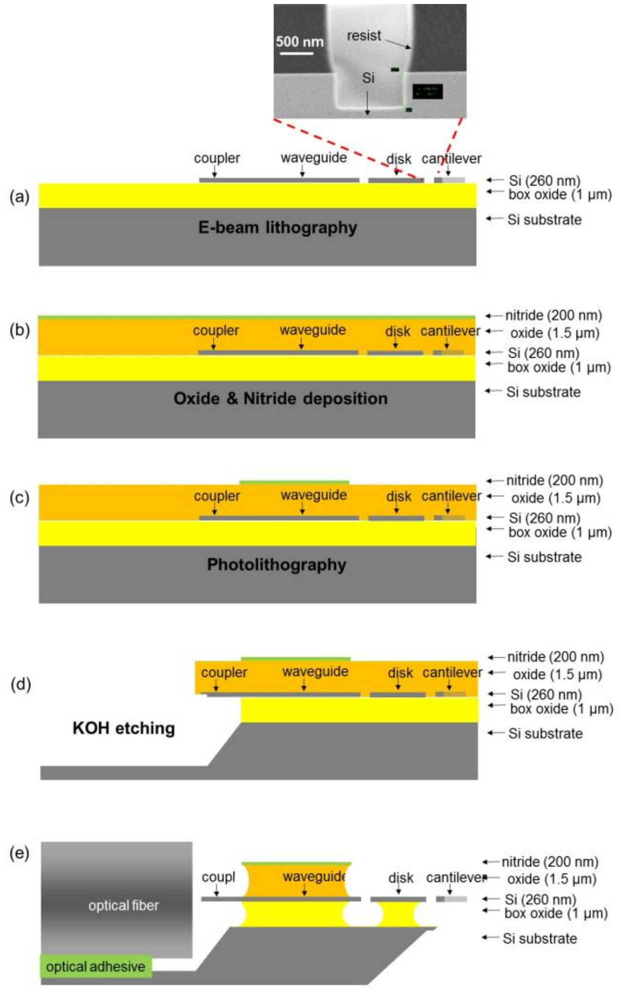


Figure 1: Nanofabrication of the optomechanical device. (a) E-beam lithography. (b) Oxide & nitride depositions. (c) Photolithography and nitride dry etch (d) Oxide and KOH etching. (e) Cantilever releasing with wet HF etching, critical point drying, mechanical and FIB under-cut below the cantilever, and gluing the cleaved optical fiber. Inset shows sidewall profile from the Si etch, scale bar 500 nm.

An, Sang M.; Zou, Jie; Holland, Glenn; Chae, Jungseok; Centrone, Andrea; Aksyuk, Vladimir.
"Optomechanical transducer-based soft and high Frequency nanoscale cantilever for atomic force microscopy."
Paper presented at the Solid State Sensor, Actuator and Microsystems Workshop, Hilton Head Island, SC, Jun 5-9, 2016.

multiple contact optical lithography steps are combined for defining device layers. This work is focused on device demonstration, and uses a few steps that are not compatible with batch fabrication. A much more sophisticated process aimed at batch fabrication of a wide class of similar devices is reported in a separate paper at this conference.

In the first step, E-beam lithography is used to define all features in the SOI Si, with critical features being the narrow gaps and the small cantilever width, followed by inductively-coupled plasma reactive ion etching for patterning the Si layer with a C_4F_8 passivation-based SF_6 etching technique [9] as shown in Fig. 1(a). Note that we check the etched vertical profile with a test silicon chip which has 1 μm line pattern before device etching, as depicted in the inset of Fig. 1(a). We realize vertical and very smooth sidewall profiles, which are required for controlling optical mode shapes and achieving the high optical quality factor for high sensitivity and selectivity for in-plane mechanical motion.

Next step is the low-pressure chemical vapor deposition (LPCVD) of SiO_2 and nitride as shown in Fig. 1(b). The oxide is used as optical cladding and sacrificial layer, and nitride as a mask layer for the subsequent Hydrofluoric acid (HF) release step. Nitride windows near the microdisk/cantilever and the fiber couplers are opened by photolithography and reactive ion etching, as shown in Fig. 1(c). At this point, the chip is annealed for 1 hour at 1000 °C to densify and improve the film quality of the oxide and nitride. Following this, we lithographically pattern and dry etch all layers stopping on the Si substrate to define patterns for fiber v-grooves and for chip singulation. Potassium hydroxide (KOH) etching defines 75 μm deep v-grooves. During this step, the SOI silicon is sufficiently protected by the BOX and top oxide layers as shown in Fig. 1(d).

We mechanically cleave to singulate 5 mm × 5mm die, followed by mechanical polishing of the Si die corner at 45° from the backside and focused ion beam (FIB) undercut of the transducer area to expose the cantilever probe at the chip corner (Fig. 2) and to sharpen the AFM probe tip. This mechanical processing is needed for unimpeded sample approach with the in-plane fabricated probe in AFM experiments (in the future may be accomplished by an appropriate combination of scalable back and front bulk micromachining techniques). The devices are released by wet etching in 49 % by mass HF solution in water, followed by rinsing and supercritical point drying. Figure 2(a) shows side view of the die corner after mechanical milling for gross under-cut of the Si substrate under the cantilever with 45° milling angle using diamond grit sandpaper. Figure 2(b) shows SEM side view image of a finished, FIB-milled and HF-released device.

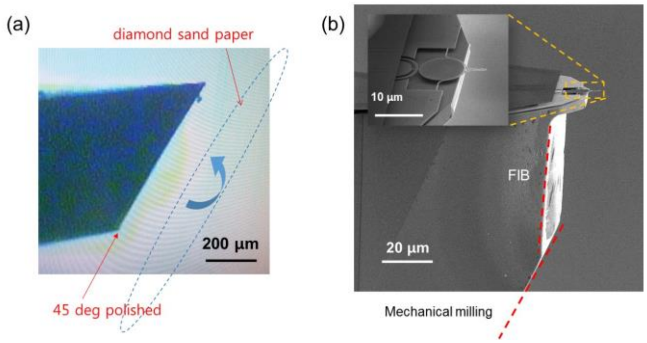


Figure 2: (a) Mechanical milling result. Si substrate under the cantilever is firstly polished by milling machine with diamond sand paper at 45 ° angle. (b) FIB milling is precisely performed near the cantilever area.

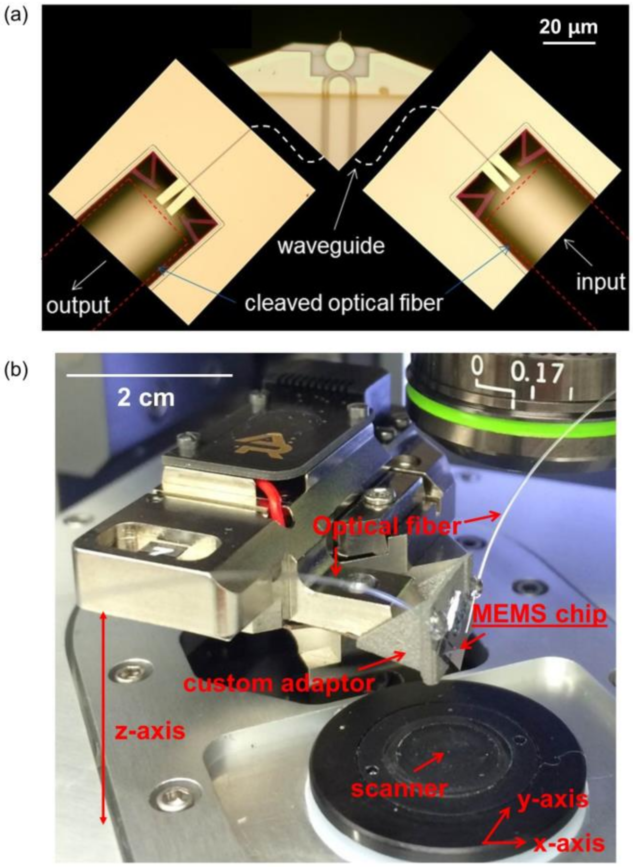


Figure 3: (a) Optical microscope images of the fabricated optomechanical device. (b) Installation of the optical fiber glued device into a commercial AFM system.

Figure 3(a) shows a top down optical microscope view of the optomechanical device and the v-groove terminations with Si waveguide optical couplers. The released die is attached with epoxy to a custom 3D-printed metal adapter and then bare, cleaved, single mode telecom optical fibers are actively aligned in the v-grooves to the on-chip inverse-taper optical couplers using a 1550 nm wavelength laser source. The fibers are glued into the v-grooves and to the adapters using ultra-violet (UV) curable epoxy. The fiber facet and the suspended Si inverse taper structure at the end of the v-grooves typically remain epoxy-free.

We install this optical fiber glued device into a commercial AFM system. We only use the chip cantilever chip holder and the sample scanner of the AFM, while our optomechanical signal is fed back into the instrument in place of its normal far-field beam-bounce optical detection system as shown in Fig. 3(b). The active corner on the die with the nanoscale sharpened probe is oriented down toward the sample stage of the AFM.

DEVICE DESIGN AND CHARACTERIZATION

Figure 4(a) shows an optical micrograph of the fabricated integrated silicon cavity optomechanical transducer with a basic schematic of the AFM measurement. The nominal fabricated disk diameter is 10 μm, while the cantilever nominal width and length are 120 nm and 24 μm, respectively; the gap between cantilever and microdisk is ≈ 200 nm, and the tip radius after FIB sharpening is ≈ 15 nm, which is comparable to the tips of commercial AFM cantilevers.

Figure 4(b) shows the working principle for a cavity optomechanical transducer-based near-field detection of cantilever motion. The mechanically-stationary microdisk is a high quality factor whispering gallery optical cavity that can be sensed through an evanescently coupled Si waveguide. Coupling into a cavity optical resonance mode results in a spectrally-narrow dip in waveguide transmission, Fig 4b. Optical quality factors of the 10 μm diameter microdisk resonator typically lie between 15 000 to 100 000 depending on the surface cleanliness of the microdisk rim, the roughness of the etched sidewall, and the geometry of the waveguide-microdisk coupling area.

The cantilever is too narrow to support a guided optical mode and to guide any light away from the optical cavity. Thus it does not affect the cavity optical loss. Instead, moving the cantilever into (out of) the evanescent fields of the cavity lowers (increases) the cavity optical resonance frequency, shifting the transmission dip. The shift of the spectrum can be translated into an amplitude modulation of the transmitted light by tuning the excitation laser to a fixed wavelength on the shoulder of the resonance, Fig. 4(b). Therefore, the photodetector voltage becomes linearly proportional to the cantilever position. Figures 5(a) and 7(b) shows that the motion readout noise is low enough to clearly resolve the thermal fluctuations of the mechanical probe itself, both when free and in contact with the sample. Therefore, the measurement performance is determined by the probe's thermal mechanical noise.

The non-contact noise spectrum for the cantilever used in the AFM experiment is shown in Fig. 5(a), measured with ≈ 3 mW of input optical power. The mechanical stiffness is estimated by finite element calculation to be ≈ 1 N/m and cantilever mass is in the sub-picogram range. The observed resonance frequency of ≈ 4 MHz agrees well with the calculation. These parameters together with the measured quality factor Q ≈ 20, are used to calibrate the sensitivity using the equipartition theorem. This gives the readout noise background in Fig. 5(a) of ≈ 7 fm/Hz$^{1/2}$ and the thermodynamic Langevin force noise density of ≈ 6 fN/Hz$^{1/2}$ acting on the cantilever, in air. Note that we can, in principle, widely vary the cantilever resonance frequency (200 kHz to 110 MHz) and stiffness (0.01 N/m to 290 N/m) by varying the design of e-beam lithography pattern [10].

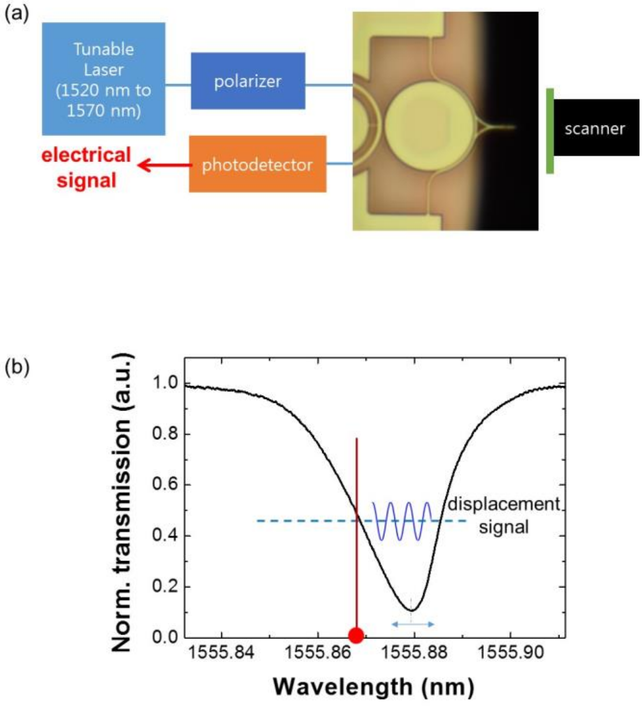


Figure 4: Optomechanical transducer-based nanoscale cantilever. (a) Device and detection schematic. (b) Working principle.

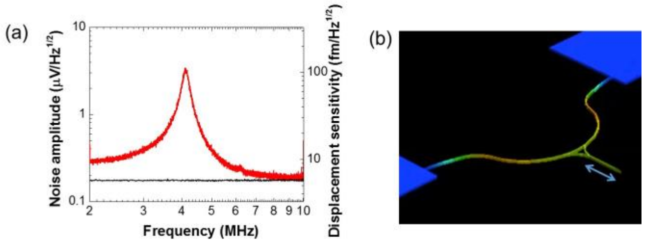


Figure 5: (a) Measured mechanical resonance frequency (4 MHz). (b) Simulation results of corresponding mechanical resonance.

This motion readout signal can be used by the AFM system as the cantilever "deflection" signal. Following conventional contact mode protocol, the AFM closes a feedback loop by adjusting the height of the probe relative to the sample to maintain deflection near a fixed setpoint value, adjusting for the changes in the sample topography as the probe is scanned.

EXPERIEMTNAL RESULTS

We performed fast scanning AFM and a PTIR measurement on a single location with the optomechanical transducer-based nanoscale cantilever.

Fast scanning

Figure 6(a) shows the contact-mode fast-scanning AFM image of a 3 μm period grating in ambient conditions. A wide area of 30 μm × 30 μm is imaged a high resolution (512 × 512 pixels) using a line scan rate of 39.06 Hz in the fast direction, which corresponds to a cantilever linear speed of 2.93 mm/s (total scan time: 13.5 s). Note that these times and frequencies properly account for the additional scanner turn-around time between each line. Even at this speed, the cantilever followed the sharp 25 nm high steps of the surface topography of the grating as shown in the Topo + Deflection images

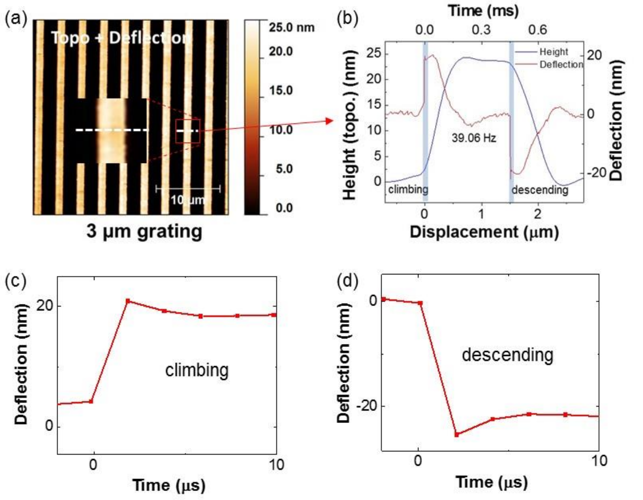


Figure 6: AFM measurement of a test grating. (a) AFM image of the 25 nm tall grating lines. (b)-(d) a single line scan. Experimental uncertainty is smaller than the data marker size.

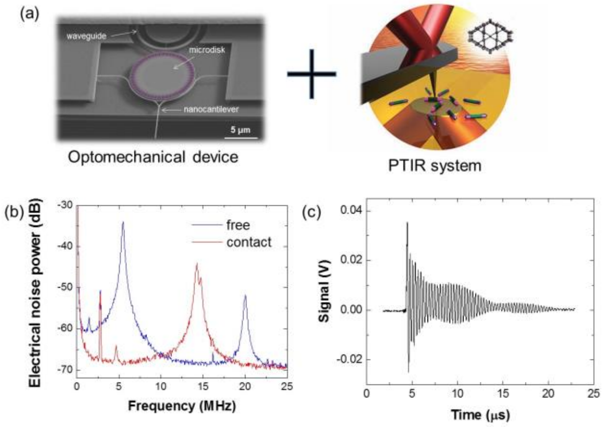


Figure 7: PTIR measurement. (a) Optomechanical probe is used instead of a conventional AFM cantilever and its beam-bounce readout in PTIR nanoscale chemically-sensitive imaging system. (b) Cantilever probe is limited by fundamental thermodynamic mechanical noise which is lower than thermal noise of conventional cantilevers in air. Noise power is relative to 1 mW. (c) Signal from a 50 nm thick PMMA film.

and line profiles in Fig. 6(b). The cantilever deflection changes very quickly at the grating steps, followed by the slower compensation by the AFM z feedback ("topography" channel). At the steps, the cantilever climbs up the wall (Fig. 6(c)) and descends the valley (Fig. 6(d)) with the response that is within about 20 % of the final value achieved within the 2 µs single time step duration. Based on the standard deviation among 10 adjacent points on a flat portion of the sample, taken at 2 µs per point, the noise per point is estimated as 20 pm one standard deviation.

PTIR measurement

We have integrated our optomechanical probe into a commercial photo-thermal induced resonance (PTIR) system [11]. PTIR combines the nanoscale resolution of AFM and optical spectroscopy and enables measuring local infrared absorption spectra and mapping chemical composition with nanoscale resolution [12,13]. The system operates by illuminating a thin-film sample with a short pulse from a tunable infrared laser. If the sample at a given location absorbs the specific infrared wavelength of the pulse, the optical energy is locally converted into heat and results in surface motion due to thermal expansion. An AFM cantilever in contact with the sample at such location experiences a mechanical "kick" which is detected. Typically, the short thermo-mechanical kick from the sample excites one or more mechanical resonant modes of the cantilever, and amplitude of the cantilever vibration ringdown provides a measure of local infrared absorption.

The exquisitely high-precision motion readout and low thermal noise of our nanoscale sensor compared to larger cantilevers in air will enable fast PTIR measurements of extremely thin samples. The low readout noise means fewer ringdown traces have to be averaged to achieve good signal-to-noise ratio at each point, and therefore faster acquisition of images and absorption spectra will be possible. By substituting our nanoscale cantilever and optical readout instead of a conventional microscale cantilever and beam-bounce readout (Fig. 7(a)), and leveraging the smaller thermomechanical and readout noises of our system (Fig. 7b), in preliminary experiments we were able to easily measure the PTIR ringdown signals from a test film of poly (methyl methacrylate) (PMMA) only about 50 nm thick (Fig. 7c) with 1024 averages.

CONCLUSION

We have integrated an optomechanical transducer-based nanoscale cantilever into AFM and PTIR systems. We demonstrate fully-functional contact mode AFM imaging with the probe, highlighting fast scanning and low noise. We further integrate the probe in a photo-thermal induced resonance system, and detect PTIR signal from a thin sample.

REFERENCES

[1] N. Kodera, D. Yamamoto, R. Ishikawa, and T. Ando, "Video imaging of walking myosin V by high-speed atomic force microscopy", Nature, 468, 72-76 (2010).

[2] M. Shibata, H. Yamashita, T. Uchihashi, H. Kandori, and T. Ando, "High-speed atomic force microscopy shows dynamic molecular processes in photoactivated bacteriorhodopsin", Nat. Nanotech. 5, 208-212 (2010).

[3] T. Uchihashi, R. Iino, T. Ando, and H. Noji, "High-Speed Atomic Force Microscopy Reveals Rotary Catalysis of Rotorless F1-ATPase", Science, 333, 755-758 (2011).

[4] K. Srinivasan, H. Miao, M. T. Rakher, M. Davanço, and V. Aksyuk, "Optomechanical Transduction of an Integrated Silicon Cantilever Probe Using a Microdisk Resonator", Nano Lett., 11(2), 791-797 (2011).

[5] D. Woolf, P.-C. Hui, E. Iwase, M. Khan, A. W. Rodriguez, P. Deotare, I. Bulu, S. G. Johnson, F. Capasso, and M. Loncar, " Optomechanical and photothermal interactions in suspended photonic crystal membranes", Opt. Exp. 21(6), 7258-7275 (2013).

[6] S. L. Portalupi, M. Galli, C. Reardon, T. F. Krauss, L. O'Faolain, L. C. Andreani, and D. Gerace, "Planar photonic crystal cavities with far-field optimization for high coupling efficiency and quality factor", Opt. Exp. 18, 16064 (2010).

[7] K. Srinivasan and O. Painter, "Linear and nonlinear optical spectroscopy of a strongly coupled microdisk–quantum dot system", Nature 450, 862-865 (2007).

[8] M. Eichenfield, C. P. Michael, R. Perahia, and O. Painter, "Actuation of micro-optomechanical systems via cavity-enhanced optical dipole forces", Nat. Photon. 1, 416-422 (2007).

[9] F. Roozeboom, F. van den Bruele, Y. Creyghton, P. Poodt, and W. M. M. Kessels, "Cyclic Etch/Passivation-Deposition as an All-Spatial Concept toward High-Rate Room Temperature Atomic Layer Etching", ECS J. Solid State Sci. Technol. 4, N5067-N5076 (2015).

[10] Y. Liu, H. Miao, V. Aksyuk, and K. Srinivasan, "Wide cantilever stiffness range cavity optomechanical sensors for atomic force microscopy", Optics Exp. 20, 18268-18280 (2012).

[11] A. M. Katzenmeyer, V. Aksyuk, and A. Centrone, "Nanoscale Infrared Spectroscopy: Improving the Spectral Range of the Photothermal Induced Resonance Technique", Anal. Chem., 85 (4), pp 1972–1979 (2013).

[12] B. Lahiri, G. Holland, V. Aksyuk, and A. Centrone, "Nanoscale Imaging of Plasmonic Hot Spots and Dark Modes with the Photothermal-Induced Resonance Technique", Nano Lett., 13, 3218–3224 (2013).

[13] A. M. Katzenmeyer, J. Canivet, G. Holland, D. Farrusseng, and A. Centrone, "Synthetic Assessing chemical heterogeneity at the nanoscale in mixed-ligand metal–organic frameworks with the PTIR technique", Angew. Chem. Int. Ed., 53, 2852–2856 (2014).

CONTACT

*V. Aksyuk, tel: +1-301-975-2867; vladimir.aksyuk@nist.gov

Characterization of Monoclonal Antibody Drug Products Using High Resolution NMR

L. W. Arbogast, R. G. Brinson, J. P. Marino
National Institute of Standards and Technology (NIST)

Purpose

High-resolution 2D ^{1}H-^{13}C and ^{1}H-^{15}N correlated nuclear magnetic resonance spectroscopy (NMR) provides a robust approach for producing unique spectral signatures of the higher order structure of protein therapeutics, including monoclonal antibodies (mAbs) at atomic resolution in solution. Such signatures can be used as a tool to establish consistency of protein folding for drug quality assessment as well as for structural comparability of related drug products.

Methods

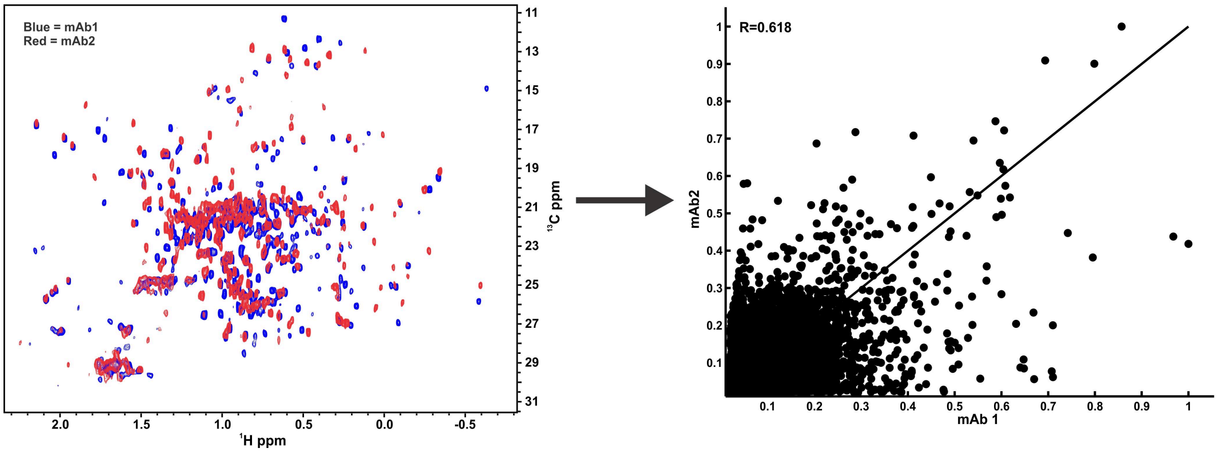
Using the IgG1κ NIST monoclonal antibody (NISTmAb), we demonstrate the acquisition of ^{1}H-^{13}C and ^{1}H-^{15}N correlated 2D NMR spectra at natural isotopic abundance using both conventional and state-of-the art rapid acquisition techniques. Furthermore, we demonstrate their use for generating unbiased statistical comparisons of mAb structure. Techniques are demonstrated on intact antibodies and protease-cleaved Fab and Fc fragments as well as intact and released mAb glycans.

Results

Results from this study indicate that 2D NMR methods are capable of statistically discriminating between dissimilar species, such as between the Fab domains of from different mAbs or between the glycosylated and variably deglycosylated Fc domains. Furthermore, statistical analysis suggests that, within the limit of detection, no significant structural differences are observed between the Fab and Fc domains of intact mAbs and their corresponding fragments, validating a domain fragment based approach for mAb HOS characterization.

Conclusion

This study demonstrates the precision and resolution with which 2D NMR techniques can be used characterize the higher order structure of protein therapeutics, including mAbs, at atomic resolution within reasonable experimental time frames and how these methods can be used to establish statistical structural comparability between drug samples.



Arbogast, Luke; Brinson, Robert; Marino, John.
“Characterization of Monoclonal Antibody Drug Products Using High Resolution NMR.”
Paper presented at the AAPS Published Meeting Abstracts, Boston, MA, May 16-May 18, 2016.

Optimizing noise for defect analysis with through-focus scanning optical microscopy

Ravikiran Attota*, John Kramar
Engineering Physics Division, PML, NIST, Gaithersburg, Maryland, 20899, USA

ABSTRACT

Through-focus scanning optical microscopy (TSOM) shows promise for patterned defect analysis, but it is important to minimize total system noise. TSOM is a three-dimensional shape metrology method that can achieve sub-nanometer measurement sensitivity by analyzing sets of images acquired through-focus using a conventional optical microscope. Here we present a systematic noise-analysis study for optimizing data collection and data processing parameters for TSOM and then demonstrate how the optimized parameters affect defect analysis. We show that the best balance between signal-to-noise performance and acquisition time can be achieved by judicious spatial averaging. Correct background-signal subtraction of the imaging-system inhomogeneities is also critical, as well as careful alignment of the constituent images used in differential TSOM analysis.

Keywords: TSOM, noise optimization, defect analysis,

1. INTRODUCTION

As the use of three-dimensional (3-D) components in nanotechnology increases, high-throughput and economical 3-D shape analysis and process monitoring of nanoscale objects is increasingly desirable[1-5] and at the same time increasingly challenging [5, 6]. Several excellent metrology tools are currently available for such a purpose [7-44], with each tool having certain advantages and disadvantages. However, it would be beneficial if metrology could be done using a widely available, low cost, tool such as a conventional optical microscope. We and other researchers have shown that this can be achieved using through-focus scanning optical microscopy (TSOM) [6, 45-56]. Furthermore, the same approach can be extended to patterned defect analysis [57, 58] and also to larger microscale targets making TSOM a valuable 3-D metrology method for targets ranging from the nanoscale to the microscale.

Application of TSOM has been demonstrated for several metrology challenges including, but not limited to: critical dimension (linewidth), overlay, patterned defect detection and analysis, FinFETs, nanoparticles, photo-mask linewidth, thin-film thickness, through-silicon vias (TSVs), high-aspect-ratio (HAR) targets and others [6, 45-55]. Though not yet published, we have also shown the applicability of TSOM for fabrication process monitoring of MEMS/NEMS devices and micro/nanofluidic channels. Sub-nanometer measurement resolution has been demonstrated [6, 49]. Three-dimensional shape analysis of isolated sub-50 nm wide lines with sub-nanometer resolution was experimentally demonstrated using visible illumination wavelength of 546 nm [6]. Measurement sensitivity of less than 0.1 nm was revealed for sub-25 nm wide lines (critical dimensions (CDs)) again using 546 nm wavelength [6]. TSOM is being increasingly recognized as a viable nanometrology method, as evidenced by being listed in several technology road maps and guides [59-61], patent applications [62, 63], and science news reports [64, 65].

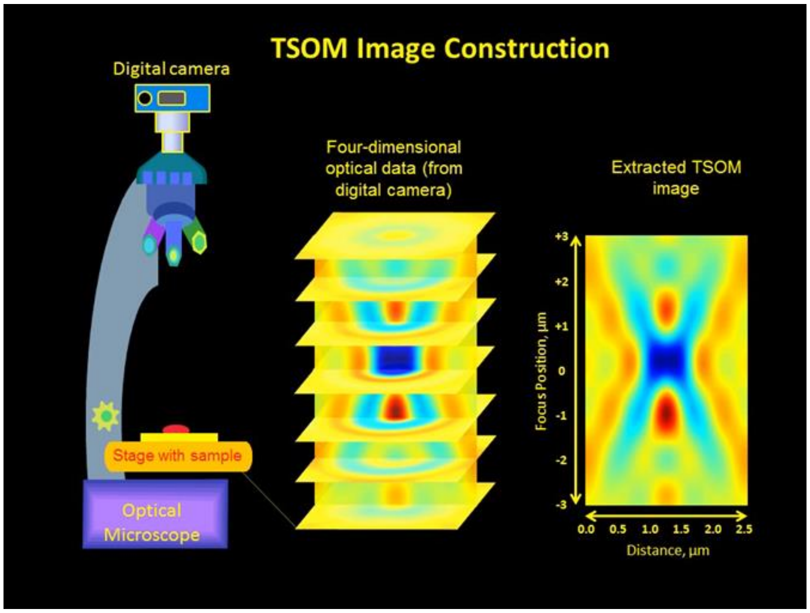
Given the increasing attention, it is important that we systematically address how to optimize the data collection and analysis conditions. Here we present common parameters that affect the noise and study how these parameters can be practically optimized for reduction of the noise. In this paper we deal only with the optical system noise. Wafer noise such as generated due to line edge roughness [66] is not included. The parameters under consideration are commonly known, but they are here applied uniquely to TSOM. Following this we demonstrate how the optimized parameters affect defect analysis.

*Ravikiran.attota@nist.gov; phone +1 301 975 5750

Updated 3/20/14

Attota, Ravikiran; Kramar, John.
"Optimizing noise for defect analysis with through-focus scanning optical microscopy."
Paper presented at SPIE Advanced Lithography, San Jose, CA, Feb 21-Feb 25, 2016.

A typical TSOM image is a cross-section constructed from the four-dimensional (4-D) optical data [49] acquired using a conventional optical microscope as a target is scanned along the focus direction [49, 52]. A multimedia figure depicting the method for constructing a TSOM image is presented in Video. 1 [52]. In the TSOM image the X (horizontal), Y (vertical), and color scale axes represent the spatial position across the target, the focus position, and the optical intensity, respectively. A differential TSOM (D-TSOM) image is produced by subtracting two TSOM images (usually obtained from two similar targets). The D-TSOM images thus produced highlight the dimensional differences down to a sub-nanometer scale [6, 49]. In addition, the D-TSOM image patterns are distinct for different types of parameter changes, but qualitatively similar for different magnitude changes in the same parameter [48, 49].



Video 1. The method for constructing a TSOM image. http://dx.doi.org/doi.number.goes.here

Optical content of a D-TSOM image provides valuable information about the 3D shape of the targets being compared, including defects. Optical content includes both the pattern created by variations in the optical signal strength and the magnitude of the optical signal itself. One of the ways to quantify the optical signal strength is by using optical intensity range (OIR), [6] defined as the absolute difference between the maximum and the minimum optical signal strength in a given TSOM image (or D-TSOM image) multiplied by 100. If the OIR of a given topographical difference (between any two targets) is safely above the noise level, then that dimensional difference can be detected with no ambiguity. However, as the magnitude of the dimensional difference decreases, there comes a point where OIR of the signal generated due to the dimensional difference is similar to or less than that of the OIR of the microscope system noise. Under these circumstances that dimensional difference cannot be detected with confidence as the signal from the noise dominates the signal from the dimensional difference. This necessitates optimal reduction, and also determination of the base level of the optical system noise. We perform this exercise in this paper.

The following method was chosen to quantify the total noise. Generate a D-TSOM image using two independently acquired and constructed TSOM images from the same target under the exact same experimental conditions. If done correctly, this process will subtract out the signal from the target and the optical signal due the presence of optical and illumination aberrations. The resultant D-TSOM image is a representation of the total system noise. It is observed that this noise is usually random in nature. The following parameters (that affect the noise) have been studied here: background signal, smoothing filter span, width of the window of analysis (explained below), camera pixels, focus step height, number of interpolation points, and optical image signal strength.

An isolated Si line (nominally 31 nm linewidth and 70 nm height) on a Si substrate was used as the target. The fabrication of the target is similar to that reported earlier [6, 49, 56]. The TSOM data were acquired using a bright-field optical microscope (Zeiss Axio Imager.Z1) in the reflection mode (focus reproducibility = ±10 nm, objective magnification = 50x, collection numerical aperture (NA) = 0.55, illumination NA = 0.157, illumination wavelength = 520 nm (narrow band-pass filtered LED light source, unpolarized, total focus range of about 25 µm)). Each analysis requires three through-focus data sets under the same experimental conditions: two datasets (essentially repeats) from the selected isolated line, and one data set from a smooth, clean Si surface. The third dataset (from the smooth Si surface) is required to remove the background signal due to the imperfections in the optical system from the two target datasets. TSOM analysis was done using software developed at NIST. The software performs the following steps to the data: normalizes each through-focus image with its own mean intensity as given in Refs. [6, 56], subtracts the through-focus background noise optical image from the target optical image at each focus-height step, selects the through-focus optical images (from the background-subtracted target image) bound by a box (as shown in Fig. 2(a)), extracts an intensity profile by averaging along the box-width “W” (Fig. 1(a)) at each focus height, constructs TSOM images by stacking the intensity profiles at their respective focus positions, interpolates, and smoothens. The normalization process (first step) eliminates the effect of overall image intensity variations, if present. The two processed TSOM images obtained in this way are then cross-correlated in both horizontal and vertical directions to achieve the best aligned position. They are then subtracted to obtain D-TSOM images. This process is shown as a flow chart in Fig.1.

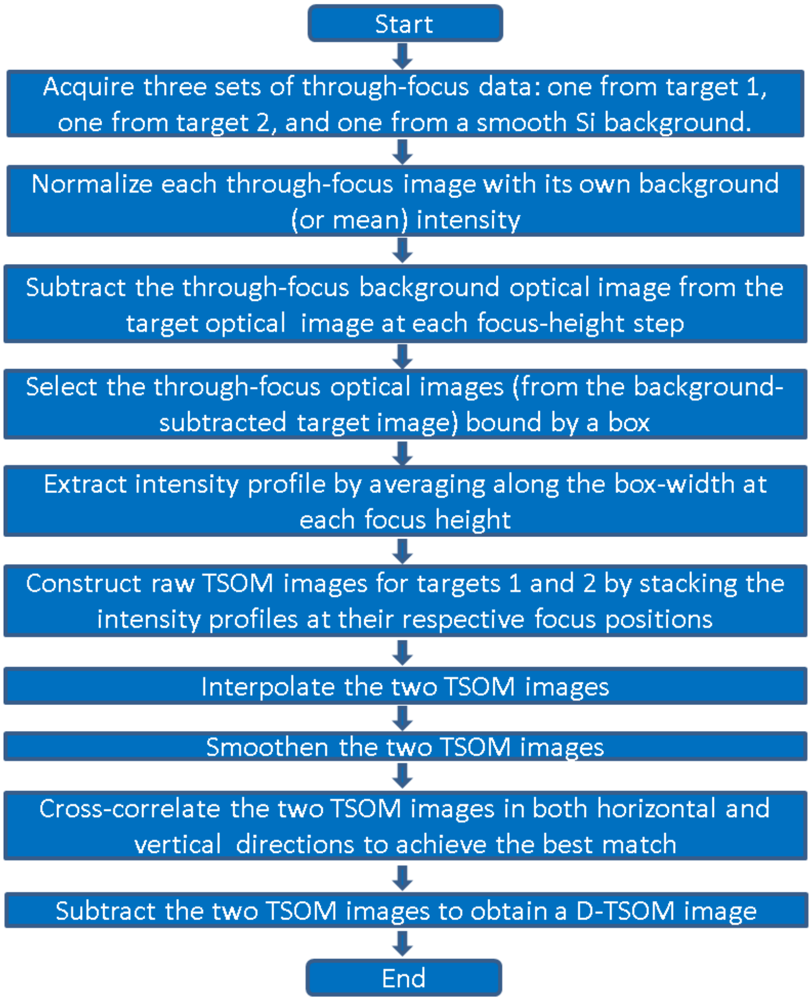

Start
Acquire three sets of through-focus data: one from target 1, one from target 2, and one from a smooth Si background.
Normalize each through-focus image with its own background (or mean) intensity
Subtract the through-focus background optical image from the target optical image at each focus-height step
Select the through-focus optical images (from the background-subtracted target image) bound by a box
Extract intensity profile by averaging along the box-width at each focus height
Construct raw TSOM images for targets 1 and 2 by stacking the intensity profiles at their respective focus positions
Interpolate the two TSOM images
Smoothen the two TSOM images
Cross-correlate the two TSOM images in both horizontal and vertical directions to achieve the best match
Subtract the two TSOM images to obtain a D-TSOM image
End

Fig. 1. Flow chart showing the steps to obtain a D-TSOM image. In this case the targets 1 and 2 are the same (repeats) and hence the D-TSOM image will be a noise D-TSOM image.

We have arrived at the following optimized conditions (or processes) for our current experimental setup based on the noise analysis and practical limitations [56]: background signal must be subtracted, box-width for analysis W = 1 μm, camera pixels = 694x520 (65 nm/pixel), focus step height = 300 nm, interpolated pixel size = 20 nm/pixel, smoothing filter span = 400 nm, and mean optical image signal strength = 100 A.U. (Arbitrary Unit). Of course, some variation in the optimized parameter values is likely depending on the specific experimental setup, measurement needs and personal judgement. In the following paragraphs we study the individual effect of each parameter on the noise by keeping the other parameters fixed. The OIR values provided are averages from 5 independent measurements. Mean OIR Standard deviations of all the TSOM images and all the D-TSOM images calculated for this study are about 1.4 % and 9 %, respectively.

Background signal removal has a profound effect on the TSOM image noise. In Figs. 2(a) and (b) we show optical images at approximately the best focus position for the target and for the smooth Si surface (which serves as the background signal image), respectively. No dramatic change can be observed in the background image subtracted target image (Fig. 2(c)), except for a change in the optical intensity scale. However, a dramatic change can be observed in the TSOM image after performing this operation. Raw TSOM images of the target (Fig. 2(d)) and the background signal (Fig. 2(e)) show background signal (or microscope noise) as streaks running from top to bottom. These streaks are completely removed in the background signal subtracted raw TSOM image (Fig. 2(f)). The subsequent image processing steps performed on the raw TSOM image remove pixelation (Fig. 2(g)). However, they also result in a loss in OIR (i.e. optical signal strength, which is essentially the absolute range of the color scale bar on the right side of the image) from 21.5 to 12.3. But this process is necessary for a meaningful analysis. Any method that satisfactorily removes pixelation can be adopted. Variations in the optical intensity profiles at the different focus positions (Fig. 2(h)) and relative orientations of the optical image plane with respect to the TSOM image plane (Fig. 2(i)) are provided for better visualization of the TSOM images.

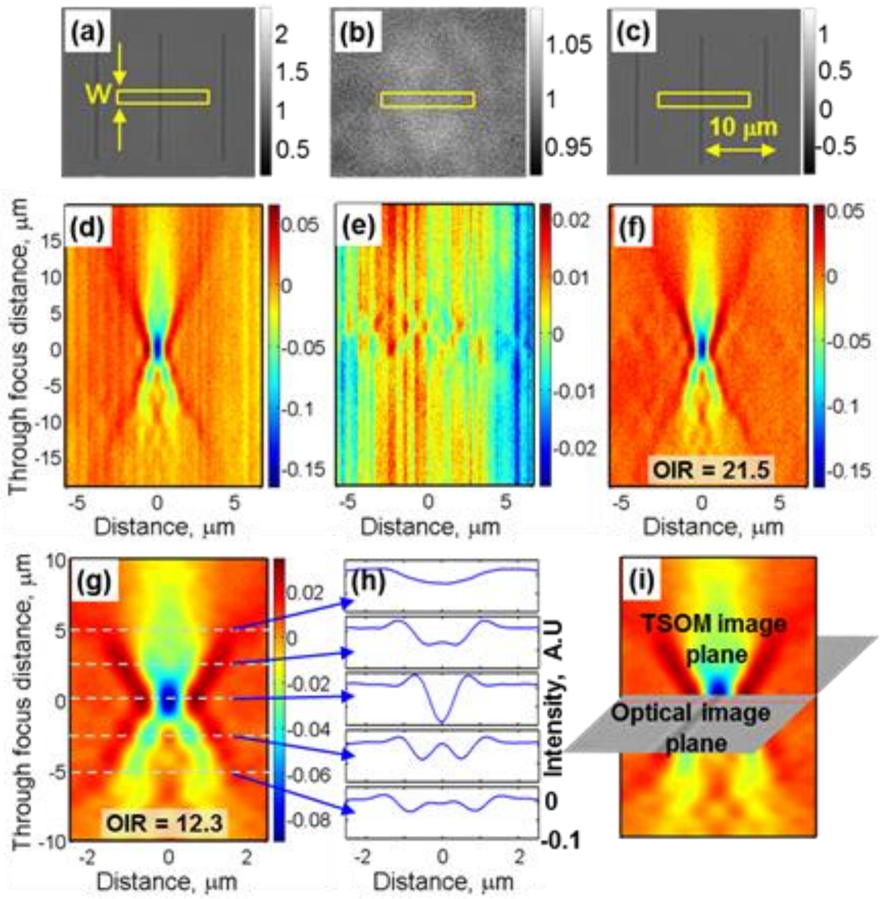


Fig. 2. Raw optical images of (a) the target, (b) a smooth Si surface, which serves as the background signal, and (c) the background-signal-subtracted target. The box shows the area selected for analysis. Raw TSOM images of (d) the target, (e) the background signal and (f) the background-signal-subtracted target. (g) The processed TSOM image. (h) Intensity profiles at the dotted lines shown in (g), and (i) optical and TSOM image planes showing their relative orientations.

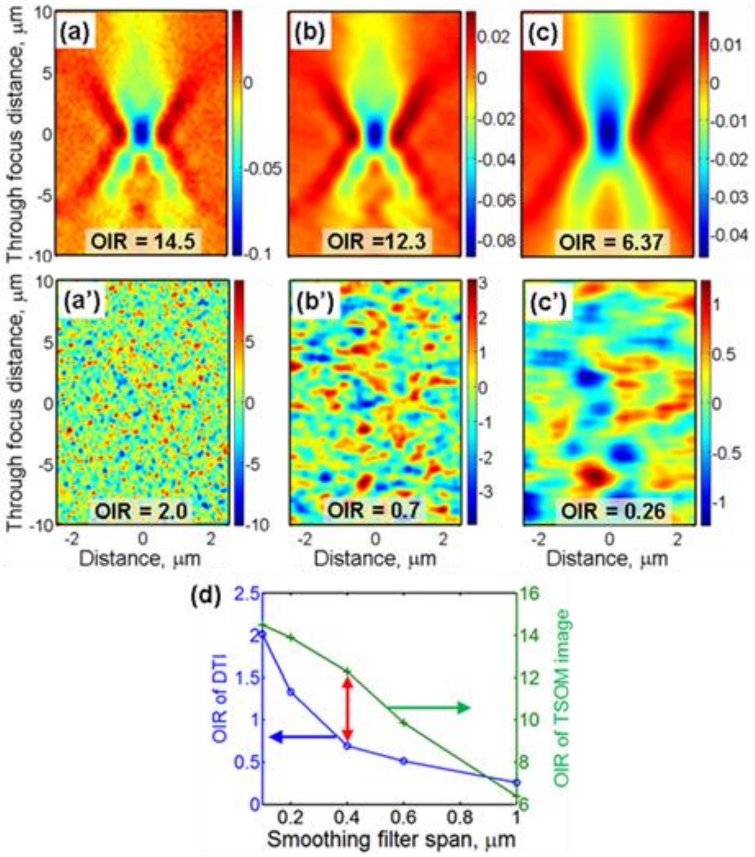


Fig. 3. (a), (b), and (c) TSOM images; and (a'), (b'), and (c') the D-TSOM images showing noise for spans of 0.1 µm, 0.4 µm, and 1.0 µm, respectively. (d) A summary plot showing the effect of moving-average span on OIRs of the TSOM images and the noise D-TSOM images as a function of the smoothing filter span. The red double arrow indicates the span selected.

Smoothing the intensity profiles is a critical step for reducing noise. Even though there are several possible smoothing methods, to demonstrate the process we here apply the moving-average method independently both in the horizontal and the vertical directions. The span of the moving-average is the variable that needs to be optimized. The span determines the number of points (or pixels) over which the averaging is performed. Initial smoothing was performed at half the nominal span length first in the horizontal direction followed by in the vertical direction. In the second step the same process was repeated at the full span length, completing the smoothing process. Smoothing significantly affects the OIR and also the noise. The TSOM image that is not smoothed shows a high OIR, but at the same time has excess pixel noise (Fig. 3 (f)), which interferes with repeatable analysis. A small span length of 0.1 µm still results in a pixelated TSOM image (Fig. 3(a)), even though the OIR decreases significantly from 21.5 to 14.5. The D-TSOM image showing noise has a large OIR of 2.0 (Fig. 3(a')). A four-fold increase in the span length from 0.1 µm to 0.4 µm reduces the OIR of the TSOM image by a small amount (from 14.5 to 12.3, Fig. 3(b)), but it significantly reduces the noise OIR from 2.0 to 0.7 (Fig. 3(b')). Further increase in the span length to 1.0 µm significantly distorts the TSOM image (Fig. 3(c)) and hence is over smoothed for most purposes, even though the noise OIR has a further reduced value of 0.26 (Fig. 3(c')). A summary of these results is plotted in Fig. 3(d). The goal here is to maximize the TSOM image signal strength (i.e., the OIR of the TSOM image) and minimize the noise (i.e., the OIR of the noise D-TSOM image) while at the same time minimizing distortion in the TSOM image. We aim to get a noise OIR of less than 1. In the current study, a span length of 0.4 µm satisfies these conditions, and hence it was selected as the optimized span length.

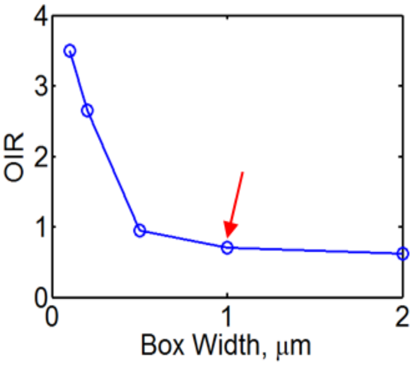


Fig. 4. Effect of the box-width 'W' (Fig. 2(a)) on the noise OIR. The red arrows indicate the selected optimized values.

It is important to note that in the D-TSOM images (Figs. 3(a'), (b'), and (c')) no residual optical signal from the line can be detected. They appear to be dominated by purely noise indicating that the other parameters selected and cross-correlation performed to obtain the D-TSOM images are well-chosen.

We turn now to the effect of box-width "W" (as shown in Fig. 2(a)), which is related to the number of profiles that are averaged to get a mean intensity profile. In Fig. 4 we plot the effect of box width on the noise OIR. As expected, smaller widths result in higher noise. The plot shows that widths in the range of 0.5 μm to 2 μm provide a noise OIR of less than 1. From this range we chose 1 μm, but it could also be 0.5 μm.

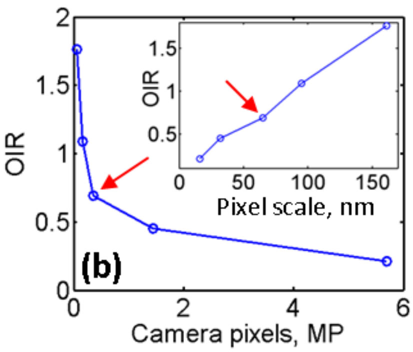


Fig. 5. Effect of the camera pixels on the noise OIR. The inset shows the same data plotted as a function of pixel scale. The red arrows indicate the selected optimized values.

The digital monochrome camera used has a native pixel count of 1040x1388 (1.44 MP). Under the magnifications used, this results in a scale of 32 nm/pixel in the digital image. Different pixel counts (pixel scale) can be achieved by pixel-binning which has two opposing effects. Binning increases signal-to-noise ratio of cameras, but it also reduces image resolution (reduces pixel count). For image analysis the former is beneficial, but the latter is detrimental. In this study we varied the illumination source intensity to maintain the image signal strength at the same level for the different pixel-binning levels selected. In this way we could study only the effect of pixel count on the noise. Different pixel counts of 208x276 (0.057 MP, 161 nm/pixel), 346x462 (0.16 MP, 95 nm/pixel) and 520x694 (0.36 MP, 65 nm/pixel) were achieved by pixel-binning. A large pixel count of 2080x2776 (5.7 MP, 16 nm/pixel) was also obtained by using the CCD sensor's piezo-scanning feature of the camera. OIR of the noise plotted as a function of the pixel count shows a continuous decrease in the noise OIR with increased pixel count (Fig. 5). The same data plotted as a function of the pixel scale (inset of Fig. 5) shows a nearly linear decreasing trend in the noise OIR with the decreasing pixel scale. This clearly demonstrates the benefit of using high pixel count in reducing the noise. Based on the less-than-1 noise OIR criteria we chose the 520x694 pixel count which produces a noise OIR of 0.7. However, if the noise needs to be reduced further, a higher pixel count could be selected (for example 2080x2776 pixels). But in this case it would require 16 times more disk storage space compared to 520x694 pixel count and also has a disadvantage of slower processing of the data. Practical feasibility also needs to be considered in selecting the optimum pixel count.

Interpolation can be used as a means of artificially increasing the pixel count. In the above pixel count study, an interpolated pixel scale (using spline method) of approximately 20 nm/pixel was maintained irrespective of the image pixel count (except for the 2080x2776 pixel count where it was 16 nm/pixel). Here we present the effect of varying interpolated pixel scale for the 520x694 pixel count (65 nm/pixel). A plot of the noise OIR as a function of the interpolated pixel scale also shows a decreasing trend in the noise with decreasing interpolated pixel size (Fig. 6(a)). From this we chose a 20 nm pixel size (shown by an arrow in Fig 6(a)). This results in a smooth TSOM image and a noise OIR much less than 1 (Figs. 3(b) and 3(b')). Technically we could choose 32 nm/pixel scale also as it results in a noise OIR less than 1. However, a larger interpolated pixel size has undesirable effect of residual intensity (color pattern) in the D-TSOM images. For example, at 65 nm/pixel scale (no interpolation) a residual color pattern in the D-TSOM image can be clearly seen as highlighted by a circle in Fig. 6(b). This is due to imperfect alignment for cross-correlation that is limited by the large pixel size. Any pixel size (either original or interpolated) that produces a residual color pattern should be avoided as much as possible. The interpolation primarily has the benefit of decreasing noise while using larger-pixel-size images (smaller stored image sizes). However, the reduction in noise is not as good as acquiring images directly at a smaller pixel scale. For example, images acquired directly at 16 nm/pixel scale show a noise OIR of 0.21 (from Fig. 5), while at the similar interpolated pixel scale noise OIR has a value of about 0.65 (from Fig. 6(a)), which is nearly three times the former. At the same time the interpolation has the benefit of reducing the noise OIR from 1.03 to 0.55 (Fig. 6(a)).

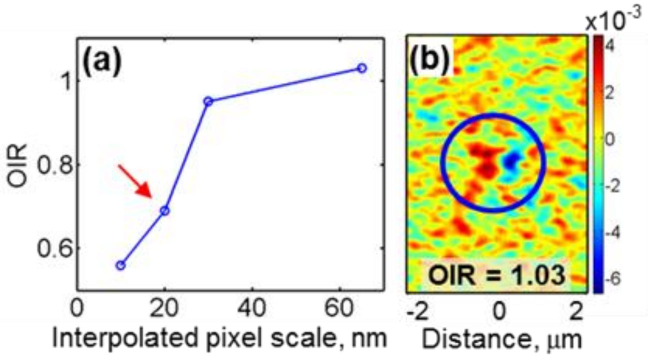


Fig. 6 (a) Effect of the interpolated pixel scale on the noise OIR. (b) A D-TSOM image showing the residual optical content (highlighted by a circle) due to imperfect cross-correlation as a result of a large scale of 65 nm/pixel.

Optical image signal strength also has a strong influence on the noise level. Under a given set of experimental conditions, a combination of illumination source intensity and the camera exposure time determines the image signal strength. Here we varied the camera exposure time to obtain the different image signal strengths. Mean image signal strength was calculated from the set of through-focus images obtained using a smooth Si background surface. The data presented here was collected at a higher source intensity compared to the other data presented earlier. As shown in Fig. 7, noise OIR decreases with increased image signal strength. This suggests that higher image signal strengths are desirable to reduce the noise level.

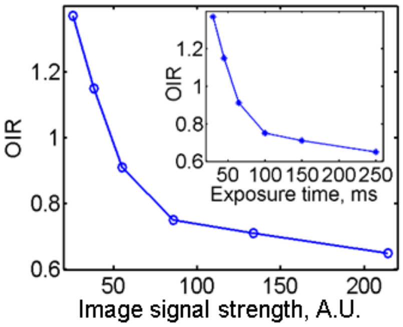


Fig. 7 Effect of the optical image signal strength on the noise OIR. The inset shows the same data as a function of the camera exposure time.

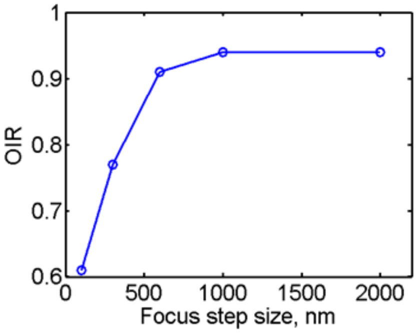


Fig. 8. Effect of the focus-step size on the noise OIR.

Similar to pixel scale (Fig. 3), focus-step size shows increased noise with increased step size as shown in Fig. 8. However, unlike pixel scale, the noise tapers out above 1000 nm step size under the current experimental conditions (this data was collected at a mean Si background image irradiance of 90 A.U.). As far as noise is concerned, any step size results in below 1 noise OIR. However, D-TSOM images appear distorted for larger step sizes and hence we chose a step size of 300 nm.

As an example, here we present the effect of optimizing parameters on the detectability of a patterned defect. To demonstrate this, we selected a 7 nm, Type-A patterned defect as shown in Fig. 9(a). Optical simulations show that this patterned defect has an OIR (or the defect signal strength) of 1.8 as shown in Fig. 9(b) [58, 67]. We need noise signal at λ = 246 nm (where the optical simulations were obtained) to demonstrate the effect of noise. However, at present we do not have access to it. As a compromise, we created different-magnitude experimental noise at λ = 520 nm using box-width as the parameter, and used this noise for defect detectability test. Box-width values of 2.0 μm and 0.4 μm produced low and high noise OIRs of 0.8 and 1.9, respectively (Figs. 9(c) and 9(d)). Adding the experimentally obtained noises (Figs. 9(c) and 9(d)) to the simulated noise-less defect signal (Fig. 9(b)) results in Figs. 9(e) and 9(f), demonstrating the effect of (artificial) noise on the defect detectability. The defect has a much better chance of detectability with a low noise (Fig. 9(e)) as we can still observe the characteristic defect pattern. On the other hand, a high noise signal makes it much harder to detect the defect (Fig. 9(f)). This demonstrates the importance of reducing the TSOM and D-TSOM image noise by optimizing the acquisition and data processing parameters so that the limits of defect detection can be extended to smaller size defects.

In summary, we have here presented the steps we typically use to process through-focus optical data for the TSOM method of analysis. We have also demonstrated practical ways to reduce noise while retaining the key information. We have studied the effect of parameters such as background signal, smoothing filter span, width of the window of analysis, camera-pixel size, focus-step height, number of interpolation points, and optical image signal strength on the noise signal strength (OIR). The parameters can be adjusted to suit individual needs, but the values provided here can serve as a guide for a starting point. For a new type of sample or analysis, or under a new set of conditions, we usually strive to achieve a noise OIR of less than 1. It is wise to perform the noise test often to monitor the continued integrity of the measurement and analysis process.

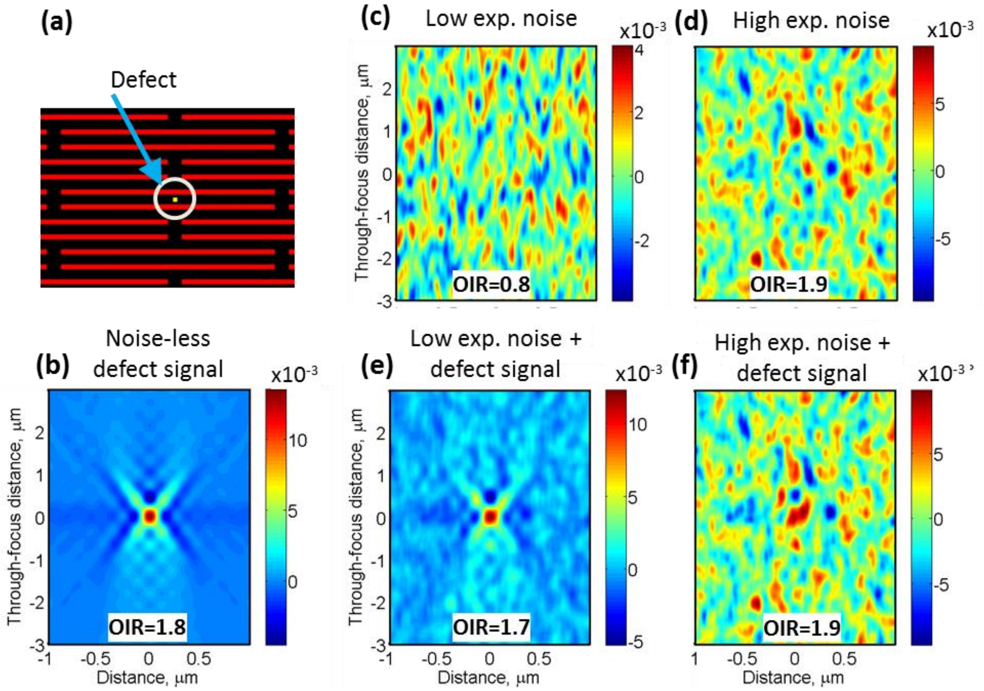


Fig. 9. (a) Type A patterned defect (defect size = 7 nm, CD = 7 nm, Pitch = 21 nm, λ = 248 nm, Si material). (b) Simulated noise-less, D-TSOM image of the defect in (a). (c) Low-noise obtained experimentally using a box-width of 1.9 μm. (d) High-noise obtained experimentally using a box-width of 0.4 μm. (e) Combined noise-less defect signal with low-noise. (f) Combined noise-less defect signal with high-noise.

Disclaimer: Any mention of commercial products or entities in this paper is for informational purposes only; it does not imply recommendation or endorsement by NIST.

Acknowledgement: The author would like to thank Richard Kasica of CNST, for providing the sample.

REFERENCES

[1] G. B. Picotto, L. Koenders, and G. Wilkening, “Nanoscale metrology,” Measurement Science and Technology, 20(8), 080101 (2009).

[2] G. Häusler, and S. Ettl, [Limitations of Optical 3D Sensors] Springer Berlin Heidelberg, 3 (2011).

[3] K. L. Richard, B. Robert, B. Theresa *et al.*, “The European nanometrology landscape,” Nanotechnology, 22(6), 062001 (2011).

[4] G. Berkovic, and E. Shafir, “Optical methods for distance and displacement measurements,” Advances in Optics and Photonics, 4(4), 441-471 (2012).

[5] A. Vaid, A. Elia, G. Iddawela *et al.*, “Hybrid metrology: from the lab into the fab,” Journal of Micro/Nanolithography, MEMS, and MOEMS, 13(4), 041410-041410 (2014).

[6] R. Attota, B. Bunday, and V. Vartanian, “Critical dimension metrology by through-focus scanning optical microscopy beyond the 22 nm node,” Applied Physics Letters, 102(22), (2013).

[7] H. Schroettner, M. Schmied, and S. Scherer, “Comparison of 3D surface reconstruction data from certified depth standards obtained by SEM and an infinite focus measurement machine (IFM),” Microchimica Acta, 155(1), 279-284 (2006).

[8] C. Wang, R. L. Jones, E. K. Lin *et al.*, “Small angle x-ray scattering measurements of lithographic patterns with sidewall roughness from vertical standing waves,” Applied Physics Letters, 90(19), 193122 (2007).

[9] T. M. Bao, L. Mininni, and D. Dawson, “Improving Sidewall Profile Metrology with Enhanced 3D-AFM,” Lithography Asia 2008, 7140, (2008).

[10] J. A. Kramar, R. Dixson, and N. G. Orji, “Scanning probe microscope dimensional metrology at NIST,” Measurement Science & Technology, 22(2), (2011).

[11] N. G. Orji, R. G. Dixson, A. E. Vladar *et al.*, “Strategies for Nanoscale Contour Metrology using Critical Dimension Atomic Force Microscopy,” Proceedings of SPIE, 8105, 810505 (2011).

[12] J. Carrero, and G. Percin, “Accurate Optical CD Profiler Based On Specialized Finite Element Method,” Proceedings of SPIE, 8324, 83240P (2012).

[13] G. L. Dai, W. Hassler-Grohne, D. Huser *et al.*, “New developments at Physikalisch Technische Bundesanstalt in three-dimensional atomic force microscopy with tapping and torsion atomic force microscopy mode and vector approach probing strategy,” Journal of Micro-Nanolithography Mems and Moems, 11(1), (2012).

[14] A. E. Vladar, P. Cizmar, J. S. Villarrubia *et al.*, “Can We Get 3D CD Metrology Right?,” Proceedings of SPIE, 8324, 832402 (2012).

[15] H. Chouaib, and Q. Zhao, “Nanoscale optical critical dimension measurement of a contact hole using deep ultraviolet spectroscopic ellipsometry,” Journal of Vacuum Science & Technology B, 31(1), (2013).

[16] J. Li, O. Kritsun, P. Dasari *et al.*, “Evaluating Scatterometry 3D Capabilities for EUV,” Proceedings of SPIE, 8681, 86810S (2013).

[17] J. Qin, R. M. Silver, B. M. Barnes *et al.*, “Fourier domain optical tool normalization for quantitative parametric image reconstruction,” Applied Optics, 52(26), 6512-6522 (2013).

[18] D. F. Sunday, M. R. Hammond, C. Q. Wang *et al.*, “Three-dimensional x-ray metrology for block copolymer lithography line-space patterns,” Journal of Micro-Nanolithography Mems and Moems, 12(3), (2013).

[19] A. Yamaguchi, T. Ohashi, T. Kawasaki *et al.*, “Three-dimensional profile extraction from CD-SEM image and top/bottom CD measurement by line-edge roughness analysis,” Proceedings of SPIE, 8681, 86812Z (2013).

[20] R. Chao, K. K. Kohli, Y. L. Zhang *et al.*, “Multitechnique metrology methods for evaluating pitch walking in 14 nm and beyond FinFETs,” Journal of Micro-Nanolithography Mems and Moems, 13(4), (2014).

[21] Y. S. Ku, “Spectral reflectometry for metrology of three-dimensional through-silicon vias,” Journal of Micro-Nanolithography Mems and Moems, 13(1), (2014).

[22] R. M. Silver, B. M. Barnes, N. F. Zhang *et al.*, “Optimizing Hybrid Metrology through a Consistent Multi-Tool Parameter Set and Uncertainty Model,” Proceedings of SPIE, 9050, 905004 (2014).

[23] A. Vaid, C. Osorio, J. Tsai *et al.*, “Hybrid metrology universal engine: co-optimization,” Proceedings of SPIE, 9050, 905009 (2014).

[24] A. E. Vladar, J. S. Villarrubia, J. Chawla *et al.*, “10 nm Three-Dimensional CD-SEM Metrology,” Proceedings of SPIE, 9050, 90500A (2014).

[25] X. X. Zhang, H. Zhou, Z. H. Ge *et al.*, “Addressing FinFET metrology challenges in 1x node using tilt-beam critical dimension scanning electron microscope,” Journal of Micro-Nanolithography Mems and Moems, 13(4), (2014).

[26] X. X. Zhang, P. Snow, A. Vaid *et al.*, “Solving next generation (1X node) metrology challenges using advanced CDSEM capabilities: tilt, high energy and backscatter imaging,” Proceedings of SPIE, 9424, 94240G (2015).

[27] Y.-M. Lee, J.-H. Li, P. C. W. Ng *et al.*, “Efficient scattering simulations for equivalent extreme ultraviolet mask multilayer structures by modified transmission line theory and finite-difference time-domain method,” Journal of Micro/Nanolithography, MEMS, and MOEMS, 9(4), 043003-043003-15 (2010).

[28] T. F. Crimmins, "Wafer noise models for defect inspection." 7971, 79710E-79710E-6.

[29] A. Vaid, B. B. Yan, Y. T. Jiang *et al.*, “Holistic metrology approach: hybrid metrology utilizing scatterometry, critical dimension-atomic force microscope and critical dimension-scanning electron microscope,” Journal of Micro/Nanolithography, MEMS, and MOEMS, 10(4), 043016-043016-13 (2011).

[30] J. Ahn, B. Lee, D.-R. Lee *et al.*, "Optical analysis on the wafer defect inspection for yield enhancement." 8681, 86811E-86811E-7.

[31] S. Godny, M. Asano, A. Kawamoto *et al.*, "Hybrid approach to optical CD metrology of directed self-assembly lithography." 8681, 86812D-86812D-8.

[32] C. J. Raymond, and Z. Li, "Photoluminescence metrology for LED characterization in high volume manufacturing." 8681, 86810P-86810P-8.

[33] J. P. Cain, N. P. Rodriguez, J. Sweis *et al.*, "A pattern-driven design regularization methodology." 9053, 905303-905303-9.

[34] K.-H. Chen, G. T. Huang, K. S. Chen *et al.*, "Improving on-product performance at litho using integrated diffraction-based metrology and computationally designed device-like targets fit for advanced technologies (incl. FinFET)." 9050, 90500S-90500S-10.

[35] K. Hitomi, S. Halle, M. Miller *et al.*, "Hybrid OPC modeling with SEM contour technique for 10nm node process." 9052, 90520W-90520W-9.

[36] Y.-S. Ku, "Spectral reflectometry for metrology of three-dimensional through-silicon vias," Journal of Micro/Nanolithography, MEMS, and MOEMS, 13(1), 011209-011209 (2014).

[37] X. Zhang, H. Zhou, Z. Ge *et al.*, "Addressing FinFET metrology challenges in 1× node using tilt-beam critical dimension scanning electron microscope," Journal of Micro/Nanolithography, MEMS, and MOEMS, 13(4), 041407-041407 (2014).

[38] R. Chao, C.-C. Liu, C. Bozdog *et al.*, "Scatterometry-based defect detection for DSA in-line process control." 9424, 942419-942419-17.

[39] M.-A. Henn, R. M. Silver, J. S. Villarrubia *et al.*, "Optimizing hybrid metrology: rigorous implementation of Bayesian and combined regression," Journal of Micro/Nanolithography, MEMS, and MOEMS, 14(4), 044001-044001 (2015).

[40] A. Starikov, and M. Sendelbach, "Special Section Guest Editorial: Control of IC Patterning Variance Part 1: Metrology, Process Monitoring, and Control of Critical Dimension," Journal of Micro/Nanolithography, MEMS, and MOEMS, 14(2), 021101-021101 (2015).

[41] L. Subramany, W. J. Chung, K. Gutjahr *et al.*, "HVM capabilities of CPE run-to-run overlay control." 9424, 94241V-94241V-7.

[42] A. Vaid, G. Iddawela, J. Tsai *et al.*, "Improved scatterometry time-to-solution using virtual reference." 9424, 94240X-94240X-9.

[43] X. Zhang, P. W. Snow, A. Vaid *et al.*, "Solving next generation (1x node) metrology challenges using advanced CDSEM capabilities: tilt, high energy and backscatter imaging." 9424, 94240G-94240G-14.

[44] R. Attota, R. M. Silver, M. Stocker *et al.*, "A new method to enhance overlay tool performance," Metrology, Inspection, and Process Control for Microlithography Xvii, Pts 1 and 2, 5038, 428-436 (2003).

[45] R. Attota, R. M. Silver, and J. Potzick, "Optical illumination and critical dimension analysis using the through-focus focus metric method - art. no. 62890Q," Novel Optical Systems Design and Optimization IX, 6289, Q2890-Q2890 (2006).

[46] R. Attota, T. A. Germer, and R. M. Silver, "Through-focus scanning-optical-microscope imaging method for nanoscale dimensional analysis," Optics Letters, 33(17), 1990-1992 (2008).

[47] R. Attota, R. G. Dixson, J. A. Kramar *et al.*, "TSOM Method for Semiconductor Metrology," Metrology, Inspection, and Process Control for Microlithography Xxv, Pt 1 and Pt 2, 7971, (2011).

[48] R. Attota, and R. Silver, "Nanometrology using a through-focus scanning optical microscopy method," Measurement Science & Technology, 22(2), (2011).

[49] R. Attota, and R. G. Dixson, "Resolving three-dimensional shape of sub-50 nm wide lines with nanometer-scale sensitivity using conventional optical microscopes," Applied Physics Letters, 105(4), (2014).

[50] M. V. Ryabko, S. N. Koptyaev, A. V. Shcherbakov *et al.*, "Method for optical inspection of nanoscale objects based upon analysis of their defocused images and features of its practical implementation," Optics Express, 21(21), 24483-24489 (2013).

[51] S. Usha, Shashikumar, P.V., Mohankumar, G.C., Rao, S.S., "Through Focus Optical Imaging Technique To Analyze Variations In Nano-Scale Indents," International Journal of Engineering Research & Technology, 2(5), 18 (2013).

[52] R. Attota, P. P. Kavuri, H. Kang *et al.*, "Nanoparticle size determination using optical microscopes," Applied Physics Letters, 105(16), (2014).

[53] M. Ryabko, S. Koptyaev, A. Shcherbakov *et al.*, "Motion-free all optical inspection system for nanoscale topology control," Optics Express, 22(12), 14958-14963 (2014).

[54] A. L. Balk, L. O. Mair, F. Guo *et al.*, "Quantitative magnetometry of ferromagnetic nanorods by microfluidic analytical magnetophoresis," Journal of Applied Physics, 118(9), (2015).

[55] M. Ryabko, A. Shchekin, S. Koptyaev *et al.*, "Through-focus scanning optical microscopy (TSOM) considering optical aberrations: practical implementation," Optics Express, 23(25), 32215-32221 (2015).

[56] R. Attota, "Noise analysis for through-focus scanning optical microscopy," Optics Letters, 41(4), (2016).

[57] A. Arceo, B. Bunday, V. Vartanian *et al.*, “Patterned Defect & CD Metrology by TSOM Beyond the 22 nm Node,” Proc. of SPIE, 8324, 83240E (2012).

[58] A. Arceo, B. Bunday, and R. Attota, “Use of TSOM for sub-11 nm node pattern defect detection and HAR features,” Proc. of SPIE, 8681, 86812G (2013).

[59] S. I. Association, [The International Technology Roadmap for Semiconductors (ITRS)] Semiconductor Industry Association, San Jose(2011).

[60] B. Bunday, T. A. Germer, V. Vartanian *et al.*, “Gaps Analysis for CD Metrology Beyond the 22 nm Node,” Metrology, Inspection, and Process Control for Microlithography Xxvii, 8681, (2013).

[61] S. E. M. I. document, [Guide for metrology techniques to be used in measurement of geometrical parameters of through- silicon vias (TSVs) in 3DS-IC structures] SEMI, (2013).

[62] S. N. KOPTYAEV, KOPTYAEV, S.N., RYABKO, M.V., Rychagov, M.N, [Optical measurement system and method for measuring critical dimension of nanostructure], USA(2013).

[63] S. N. KOPTYAEV, RYABKO, M.V., HCHERBAKOV, A.V., LANTSOV, A.D., [Optical measuring system and method of measuring critical size], USA(2014).

[64] R. Attota, Jindal, V., “Inspecting mask defects with through-focus scanning optical microscopy,”, SPIE Newsroom, (2013).

[65] M. Ryabko, Koptyev, S., Shchekin, A., Medvedev, A., “Improved critical dimension inspection for the semiconductor industry,” SPIE Newsroom, (2014).

[66] B. M. Barnes, F. Goasmat, M. Y. Sohn *et al.*, “Effects of wafer noise on the detection of 20-nm defects using optical volumetric inspection,” Journal of Micro-Nanolithography Mems and Moems, 14(1), (2015).

[67] A. Arceo, B. Bunday, V. Vartanian *et al.*, “Patterned Defect & CD Metrology by TSOM Beyond the 22 nm Node,” Metrology, Inspection, and Process Control for Microlithography Xxvi, Pts 1 and 2, 8324, (2012).

An Optomechanical Accelerometer with a High-Finesse Hemispherical Optical Cavity

Yiliang Bao, Felipe Guzmán Cervantes, Arvind Balijepalli, John R. Lawall, Jacob M. Taylor,
Thomas W. LeBrun, and Jason J. Gorman
National Institute of Standards and Technology, Gaithersburg, MD, 20899 USA
Email: gorman@nist.gov, thomas.lebrun@nist.gov

***Abstract*—A new design for an optomechanical accelerometer is presented. The design includes a hemispherical optical cavity that can achieve high finesse and a proof mass that is well-constrained by silicon nitride beams. Based on previous work and analysis, the resolution of the accelerometer will be below 1 µg/rt-Hz. Novel MEMS fabrication processes have been developed for the accelerometer that provide optimized optical and mechanical elements. The optical cavity in the accelerometer has been characterized and a tunable laser has been locked to the cavity, thereby demonstrating the possibility for closed-loop operation of the accelerometer.**

Keywords— accelerometer; MEMS; Fabry-Pérot; optical cavity

I. Introduction

This paper reports on the design, fabrication, and preliminary testing of an optomechanical accelerometer that uses Fabry-Pérot interferometry with a high-finesse optical cavity to transduce acceleration. Accelerometers typically measure the displacement of the proof mass with respect to a local reference using various techniques, including piezoelectric materials, strain gauges, and capacitive sensors. This displacement is then converted to acceleration using information about the sensor's dynamic response, such as the fundamental resonant frequency or the frequency response function. Fabry-Pérot interferometry is a highly sensitive and low uncertainty approach for measuring displacement, making it a compelling candidate for integration in accelerometers. Two mirrors are used to form an optical cavity, one being the proof mass, and a laser is used to measure the relative displacement between the two.

Fabry-Pérot interferometry has been previously demonstrated in a number of MEMS accelerometers. This work can be broken into two groups: fiber-optic cavities [1-5] and vertically oriented cavities [6-8]. The first uses an optical fiber to deliver and collect light while also serving as one mirror of the cavity. Most cavities in this group are plane parallel (i.e., two flat mirrors) although hemispherical cavities (i.e., one concave mirror) are possible [5]. Plane-parallel cavities are only marginally stable meaning that small errors in the perpendicularity of the mirrors allows light to leak from the cavity. This makes it challenging to achieve high-finesse cavities, thereby limiting the sensitivity of the accelerometer. The second group uses two mirrors in a vertical configuration and are almost always plane-parallel. However, the vertical orientation makes it easier to fabricate high quality optics.

As a result, the goal of the presented work is to develop a vertically oriented optomechanical accelerometer with a hemispherical cavity, which will be more stable than existing plane parallel cavities. This will yield a higher optical finesse and as a result, higher acceleration sensitivity. The design, fabrication, and optical testing of the accelerometer are presented in the following sections.

II. Accelerometer Design

The design of the optomechanical accelerometer is shown in Fig. 1. Two silicon chips that are fabricated separately are bonded together to make the sensor. The first chip contains a microscale hemispherical mirror that is coated with a high-reflectivity mirror coating on the concave side and an anti-reflective (AR) coating on the flat side. The second chip contains the accelerometer proof mass, which is suspended by silicon nitride beams along the top and bottom edges of the proof mass. The proof mass also has a high-reflectivity mirror coating on the side facing the mirror and an AR coating on the opposite side. There is a recess surrounding the hemispherical mirror, thereby allowing the proof mass to move perpendicular to the surface in both directions. The reflective surfaces on the mirror and proof mass form an optical cavity that can be interrogated with a laser to determine the relative displacement between these two surfaces.

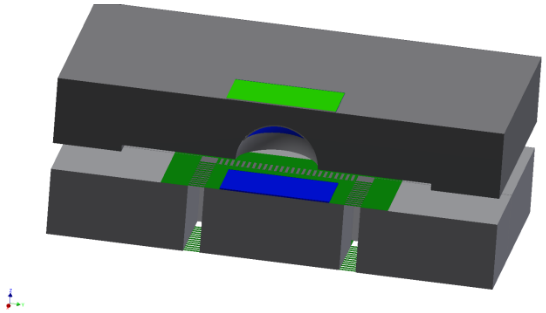


Figure 1: An exploded cross-sectional view of the optomechanical accelerometer showing the hemispherical cavity and suspended proof mass.

U.S. Government work not protected by U.S. copyright

Bao, Yiliang; Guzman, Felipe; Balijepalli, Arvind; Lawall, John; Taylor, Jacob; LeBrun, Thomas; Gorman, Jason.
"An Optomechanical Accelerometer with a High-Finesse Hemispherical Optical Cavity."
Paper presented at the IEEE International Symposium on Inertial Sensors and Systems, Laguna Beach, CA, Feb 23-Feb 25, 2016.

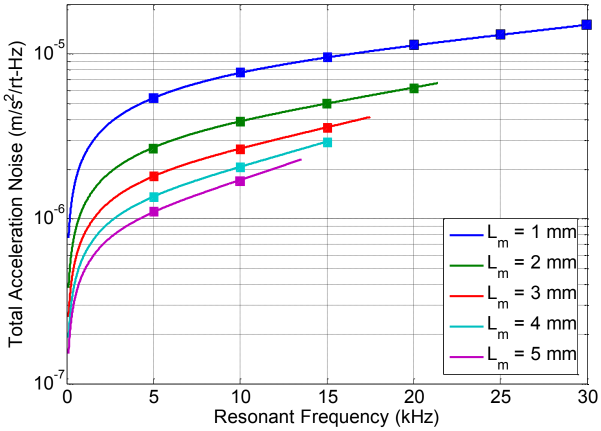


Figure 2: Calculated acceleration noise, including thermal motion and optical detection noise, for varying proof mass size. Squares indicate fabricated accelerometers.

The out-of-plane design was adopted because it allows for the fabrication of a high-quality hemispherical optical cavity that cannot easily be achieved with an in-plane accelerometer. The mechanical beam design, in which the proof mass is suspended on top and bottom, was selected to minimize the influence of rocking modes and to accentuate the piston mode or out-of-plane mode. Finite element analysis has shown that the fundamental mode is the piston mode and the first rocking mode frequencies are at least ten times higher than the fundamental. This frequency separation will result in a sensor with a simple harmonic oscillator response. Finally, with the exception of the silicon nitride beams, mirror coatings, and the AR coatings, the sensor is made of silicon and the bonding of the two chips is between silicon surfaces. As a result, this design should provide excellent thermal stability.

In order to simplify the parameter space, the following values were selected for all designs: beam width, w_b = 20 µm, beam thickness, t_b = 1.5 µm, proof mass thickness, t_m = 500 µm. The stiffness and fundamental resonant frequency are set by selecting the beam length, L_b (40 µm to 110 µm), and the length of the square proof mass, L_m (1 mm to 5 mm). The noise of the accelerometer will be dominated by the thermal noise (see [9]) and the optical detection noise. In our previous work [5], the displacement detection noise for a microscale optical cavity of similar size with a finesse of F = 1600 was found to be 2 x 10^{-16} m/rt-Hz. This is converted to acceleration noise by multiplying by the square of the fundamental natural frequency, ω_n^2. The thermal noise can be calculated using an equation in [9] and values for the proof mass, m, the quality factor, Q, which has been measured to be around 15 in air, and ω_n. Taking the root mean square of the two noise sources results in the values shown in Fig. 2 for varying L_m and ω_n. For almost all designs, the noise floor will be below 1 µg/rt-Hz (1 g = 9.81 m/s^2), demonstrating that the presented optomechanical accelerometer should result in significantly better sensitivity than most other MEMS accelerometers.

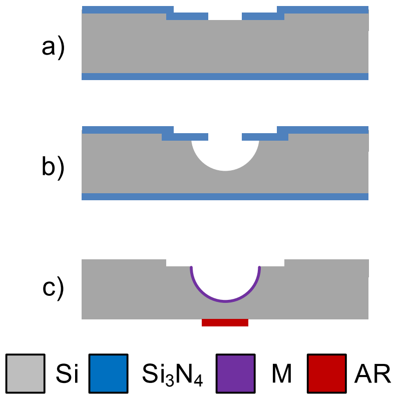


Figure 3: Fabrication process for the hemispherical mirror: a) a recess is etched in Si (DRIE) and is then coated with Si$_3$N$_4$ (LPCVD), b) aperture is etched in Si$_3$N$_4$ (RIE) and then Si hemisphere is etched (HNA), c) after removal of Si$_3$N$_4$, mirror (M) and antireflection (AR) coatings are deposited using a shadow mask and lift-off process, respectively.

In order to obtain the measurements described in Section IV, free-space optics were used to couple light into the cavity. However, we are now working on a method to assemble the two-chip system into a fiber-optic mount. The same fiber will be used to supply light to the cavity and collect the reflected light. A lens doublet at the end of the fiber will be used to optimize mode matching into the cavity. Cavity coupling will also be optimized by positioning the two-chip system at the location of highest sensitivity relative to the fiber, where it will then be set within the mount using adhesive.

III. Accelerometer Fabrication

The fabrication of the two-chip system required the development of unique processes. The hemispherical mirror chip was fabricated using a slow isotropic etch that results in low roughness and high radius of curvature. The process is described in Fig. 3. First, the recess is etched 10 µm deep using deep reactive ion etching (DRIE). The wafer is then coated with LPCVD stoichiometric silicon nitride with a thickness of 300 nm, which serves as a mask for the isotropic etch. An aperture is etched through the silicon nitride using reactive ion etching (RIE) for each hemispherical mirror. The wafer is then etched in hydrofluric, nitric, and acetic acids (HNA) for a predetermined time in order to achieve the desired depth and radius of curvature. This process is based on the one developed by Moktadir et al. [10]. However, much large apertures are used here to achieve fairly long cavity lengths (≈ 250 µm) and even larger radii of curvature (≈ 350 µm). A highly stable optical cavity is achieved through this ratio of radius of curvature to cavity length. In a final step, the mirror and AR coatings are applied through a shadow mask and lift-off resist, respectively, by an optical coatings vendor.

Fabricated mirrors are shown in Fig. 4. It is clear from the cross-sectional image (Fig. 4b) that the mirror is not a perfect hemisphere, as desired. Optical profilometer measurements were performed on mirrors to determine their surface quality, as shown in Fig. 5. The surface quality is better than λ/25 and

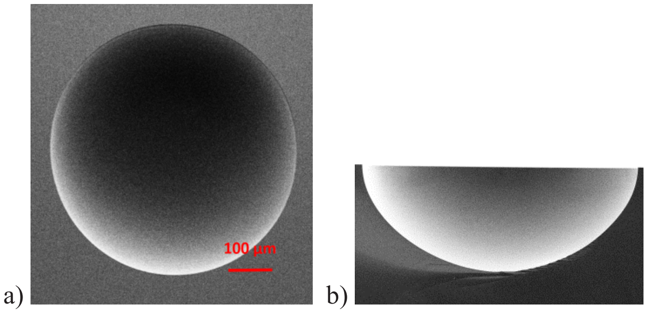


Figure 4: Etched hemispherical mirror: a) top view, b) cross-section.

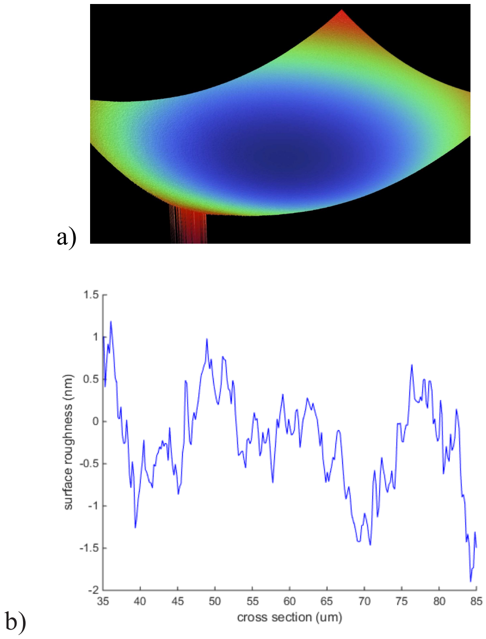


Figure 5: Optical profilometry data for a hemispherical mirror: a) 3D image, b) surface roughness.

the surface roughness is approximately 1 nm RMS, making these exceptional mirrors for interferometry. The roughness can be improved further if necessary through oxidation and etch steps.

The fabrication process for the suspended proof mass is shown in Fig. 6. First LPCVD low stress silicon nitride is deposited on a silicon wafer. The silicon nitride layer is then etched using RIE to leave patches above and below the proof mass location. Mirror and AR coatings are then applied as described above. The beam and proof mass geometry is then etched on both sides until they meet using RIE followed by DRIE. Finally the beams are released by undercutting them using KOH. A released proof mass is shown in Fig. 7.

IV. Optical Cavity Measurements

As a step towards fully functional accelerometers, the properties of the microscale optical cavities have been measured. A two-chip system with an unreleased proof mass was used for these measurements. The cavity was interrogated with a tunable diode laser with a nominal wavelength of 1550 nm. The laser was mode matched to the cavity using two lenses and the reflected light was positioned onto a photodetector using a beamsplitter. The accelerometer was positioned relative to the laser using a six-axis motion stage.

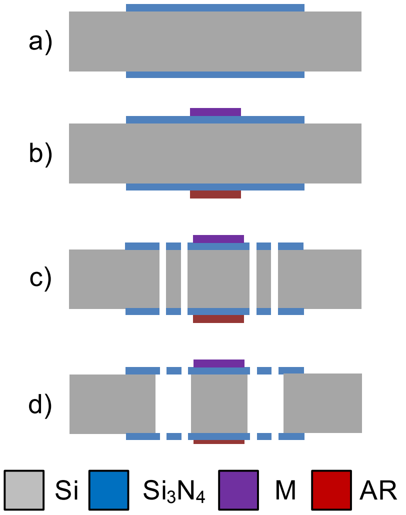


Figure 6: Fabrication process for the suspended proof mass: a) Si_3N_4 is deposited on a Si wafer (LPCVD) and patterned, b) mirror (M) and antireflection (AR) coatings are deposited using a lift-off process, c) the proof mass suspension is etched through the Si_3N_4 (RIE) and Si wafer (DRIE) on both sides, d) the remaining Si under the Si_3N_4 beams is etched (KOH).

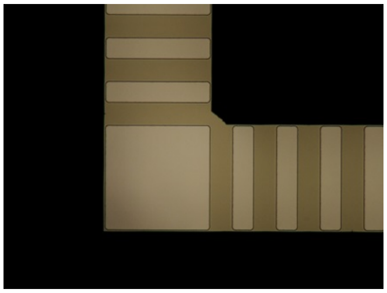


Figure 7: Transmission optical micrograph of the corner of a fabricated suspended proof mass.

After alignment, the wavelength of the laser was scanned using coarse tuning to observe the mode structure of the optical cavity. The fundamental mode is clear and repeats at a fixed interval, as expected (see Fig. 8). This interval is the free spectral range (FSR), FSR = $c/2L$, where c is the speed of light and L is the cavity length. The FSR was measured to be 678.12 GHz, indicating a cavity length of 221 µm, which is within the expected range. The finesse of the cavity is estimated to be 2798 based on a slower can of a resonance (see Fig. 8b).

While there are several ways to measure the relative displacement in the cavity, possibly the most attractive method is to lock a laser to the cavity and then measure the frequency of the laser. The laser frequency changes can then be converted to a displacement. In this work, we have used a dither lock for this purpose. The current supplied to the laser diode was modulated at a single frequency (100 kHz in this

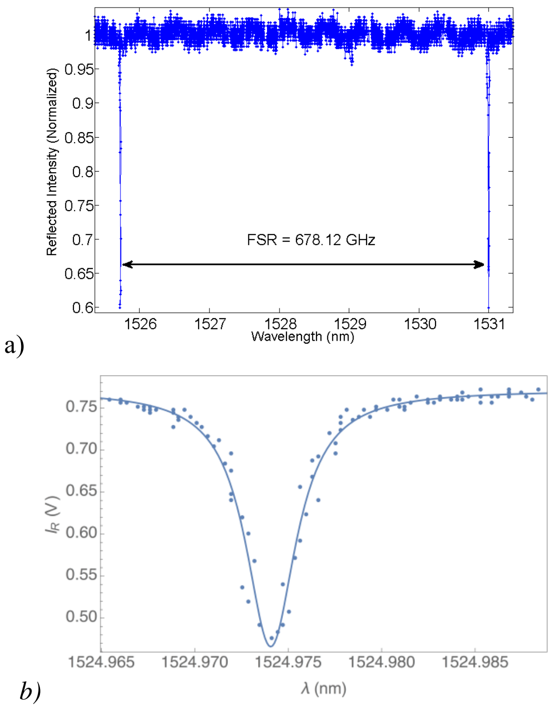


Figure 8: Reflected intensity of the hemispherical optical cavity as a function of wavelength: a) wide wavelength scan showing two adjacent optical modes, b) narrow scan showing a single mode.

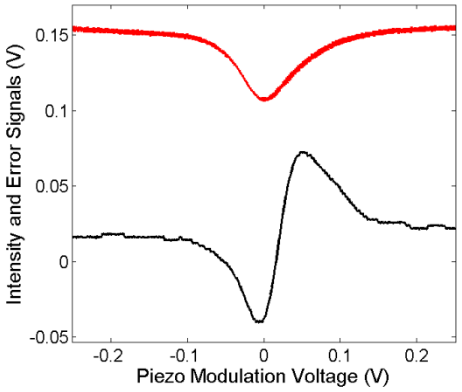


Figure 9: Optical cavity resonance (red) and error signal from lock-in amplifier (black) during a fine wavelength scan. The relationship between piezo voltage and laser frequency is approximately 10 GHz/V.

case) and the signal from the photodetector was processed by a lock-in amplifier. The output of the lock-in amplifier is an error signal that can be used for closed-loop locking of the laser to the cavity. As can be seen in Fig. 9, the error signal is the derivative of the resonance. This data was collected by using the fine wavelength scan (piezo actuator) while providing injection current modulation. The laser was successfully locked to the cavity using this error signal. However, the bandwidth of the laser controller was insufficient to do an acceleration measurement. We are currently working on an alternative approach for cavity locking that will enable optomechanical sensors with laser frequency readout.

V. Conclusions

The design and fabrication of an optomechanical accelerometer with a hemispherical optical cavity has been presented. Based on calculations, the accelerometer is expected to achieve a resolution better than 1 μg/rt-Hz for a wide range of sensor resonant frequencies, making it highly competitive compared to conventional MEMS accelerometers. The fabricated microscale concave mirrors have been shown to have excellent surface quality (better than λ/25) and very low surface roughness (1 nm RMS), thereby meeting the requirements for high-finesse optical cavities. An assembled accelerometer was found to have well-defined fundamental modes and an optical finesse around 2800. Using the dither locking technique, we were able lock a tunable diode laser to the accelerometer.

Two challenges remain before the accelerometer can be used for sensing. The first is stable fiber coupling of the microscale optical cavity. The second is dither locking of the cavity with bandwidth that exceeds that of the fundamental resonant frequency of the accelerometer (> 30 kHz) while maintaining a large tuning range (> +/- 30 GHz). These challenges are the focus of our current research.

Acknowledgment

This research was performed in part in the NIST Center for Nanoscale Science and Technology Nanofab.

References

[1] G. Schröpfer et al., "Lateral optical accelerometer micromachined in (100) silicon with remote readout based on coherence modulation," *Sens. Actuators, A*, 68, pp. 344-349, 1998.

[2] M.D. Pocha et al., "Miniature accelerometer and multichannel signal processor for fiberoptic Fabry-Pérot sensing," *IEEE Sens. J.*, 7, pp. 285-292, 2007.

[3] K. Zandi, J. A. Belanger, and Y.A. Peter, "Design and demonstration of an in-plane silicon-on-insulator optical MEMS Fabry-Pérot-based accelerometer integrated with channel waveguides," *J. Microelectromech. Sys.*, 21, pp. 1464-1470, 2012.

[4] E. Davies et al., "MEMS Fabry–Pérot optical accelerometer employing mechanical amplification via a V-beam structure," *Sens. Actuators, A*, 215, pp. 22-29, 2014.

[5] F. Guzmán Cervantes et al., "High sensitivity optomechanical reference accelerometer over 10 kHz," *Appl. Phys. Lett.*, 104, 221111, 2014.

[6] R.L. Waters and M.E. Aklufi, "Micromachined Fabry–Perot interferometer for motion detection," *Appl. Phys. Lett.*, 81, pp. 3320-3322, 2002.

[7] E.J. Eklund and A.M. Shkel, "Factors affecting the performance of micromachined sensors based on Fabry–Perot interferometry,", *J. Micromech. Microeng.*, 15, pp. 1770-1776, 2005.

[8] M.A. Perez and A. M. Shkel, "Design and demonstration of a bulk micromachined Fabry-Pérot μg-resolution accelerometer," *IEEE Sens. J.*, 7, pp. 1653-1662, 2007.

[9] T.B. Gabrielson, "Mechanical-thermal noise in micromachined vibration and acoustic sensors," *IEEE Trans. Electron Devices*, 40, pp. 903-909, 1993.

[10] Z. Moktadir et al., "Etching techniques for realizing optical micro-cavity atom traps on silicon," *J. Micromech. Microeng.*, 14, pp. S82-S85, 2004.

COVER SHEET

Temperature and Strain Measurements with Fiber Optic Sensors for Steel Beams Subjected to Fire

Yi Bao[1], Yizheng Chen[1], Matthew S. Hoehler[2], Christopher M. Smith[2], Matthew Bundy[2], and Genda Chen[1,*]

[1] Department of Civil, Architectural, and Environmental Engineering, Missouri University of Science and Technology, 1870 Miner Circle, Rolla, MO 65409, USA

[2] National Fire Research Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8666, Gaithersburg, MD 20899, USA

*Corresponding to Dr. Genda Chen. Email: gchen@mst.edu, Phone: (573)341-4462.

Bao, Yi; Chen, Yizheng; Hoehler, Matthew; Smith, Christopher; Bundy, Matthew; Chen, Genda.
"Temperature and Strain Measurements with Fiber Optic Sensors for Steel Beams Subjected to Fire."
Paper presented at the 9th International Conference on Structures in Fire SiF'16, Princeton, NJ, Jun 8-Jun 10, 2016.

ABSTRACT

This paper presents measurements of high temperatures using a Brillouin scattering based fiber optic sensor and large strains using an extrinsic Fabry-Perot interferometric sensor for assessing the thermo-mechanical behaviors of simply-supported steel beams subjected to combined thermal and mechanical loading. The distributed fiber optic sensor captures detailed, non-uniform temperature distributions that are compared with thermocouple measurements resulting in an average relative difference of less than 5 % at 95 % confidence level. The extrinsic Fabry-Perot interferometric sensor captures large strains at temperatures above 1000 °C. The strain results measured from the distributed fiber optic sensors and extrinsic Fabry-Perot interferometric sensors were compared, and the average relative difference was less than 10 % at 95 % confidence level.

INTRODUCTION

During a fire, the load capacity and stability of steel structures can significantly degrade due to adverse temperature-induced deformations and reduced material properties [1]. To assess the thermo-mechanical conditions of a structure, both temperatures and strains must be known. The current state of practice in experimental fire testing is to measure the temperature and global deformation of specimens and to use analytical models to understand the behavior of the member. Effective tools are lacking to directly measure strains in steel members subjected to fire, reliably and accurately.

Fiber optic sensors have drawn intense research interest in the past decade due to their unique advantages, such as immunity to electromagnetic interference, small size, light weight, and excellent durability and resistance to harsh environments. However, their application to structures in fire has not yet been fully explored. Conventional grating-based fiber optic sensors degrade significantly when heated over 300 °C and typically fail around 600 °C [2], which limits their application in fire. Although their temperature operation range can be increased to 1000 °C through means such as the regenerated fiber Bragg grating technique [2], the grating sensors do not provide spatially distributed measurements, but rather a point

Bao, Yi; Chen, Yizheng; Hoehler, Matthew; Smith, Christopher; Bundy, Matthew; Chen, Genda.
“Temperature and Strain Measurements with Fiber Optic Sensors for Steel Beams Subjected to Fire.”
Paper presented at the 9th International Conference on Structures in Fire SiF'16, Princeton, NJ, Jun 8-Jun 10, 2016.

measurement at the grating location. In contrast, fully-distributed fiber optic sensors provide a more detailed picture of the structural thermal field. Based on Brillouin scatterings in optical fiber, Brillouin Optical Time Domain Analysis and Brillouin Optical Time Domain Reflectometry technologies have been developed to measure strain and temperature distributions [3]. However, their spatial resolutions were typically limited to half a meter or larger, which is not precise enough in many applications. Recently, a pulse pre-pump Brillouin Optical Time Domain Analysis (PPP-BODTA) technology was developed with a 2 cm spatial resolution [4].

In this study, distributed fiber optic sensors with PPP-BODTA [5] and extrinsic Fabry-Perot interferometric (EFPI) sensors [6] are employed to measure temperatures and strains in steel beams exposed to fire. The sensors' accuracies and precisions for temperature and strain measurements are compared and evaluated.

WORKING PRINCIPLES

The working principles of the distributed fiber optic sensor and extrinsic Fabry-Perot interferometric sensor are briefly introduced in this section. In this study, all fiber optic sensors were fabricated using telecommunication-grade fused silica single-mode fibers. The fiber cross section consisted of an 8.2 μm glass core and a 125 μm glass cladding [7]. Typically, optical fibers are coated with protective polymer coatings outside of cladding to enhance the mechanical performance [8]. In this study, for strain measurement, the coatings were removed before the fibers were installed on the test specimens. However, for temperature measurement, the coatings could be left and burned off at about 300 °C to 400 °C [9].b

Distributed Fiber Optic Sensor

In this study, PPP-BOTDA based on stimulated Brillouin scatterings in optical fiber was employed. Stimulated Brillouin scatterings result from the interactions between light waves and acoustic waves in optical fiber [2]. PPP-BOTDA measures the Brillouin frequency shift along the optical fiber, which is related to the strain and temperature changes of the optical fiber. For light signals with wavelengths of 1.3 μm to 1.6 μm in single mode fibers, the Brillouin frequency shift is about 9 GHz to 13 GHz. The Brillouin frequency shift increases approximately linearly with increasing tensile strain or temperature when the temperature is not very high (< 400 °C). However, after the optical fiber is exposed to high temperatures, the linear relationships are not satisfied and must be modified [7].

Extrinsic Fabry-Perot Interferometric Sensor

An EFPI sensor typically consists of two parallel reflecting surfaces, which are separated by a cavity, as illustrated in Figure 1. Interference occurs between the multiple reflections of light between the two reflecting surfaces. The reflection spectrum of an EFPI can be described as the wavelength dependent intensity modulation of the input light spectrum [6], which is mainly caused by the optical phase difference between two reflected light beams. Constructive interference occurs if the reflected beams are in phase, and this corresponds to a high-transmission peak. If the reflected beams are out-of-phase, destructive interference occurs and this corresponds to a reflection minimum. Whether the multiply reflected beams are in phase or not depends on the wavelength (λ) of the incident light (in vacuum), the angle with which the incident light travels through the reflecting surfaces (θ), the physical length of the cavity (L) and the refractive index of the material between the reflecting surfaces (n).

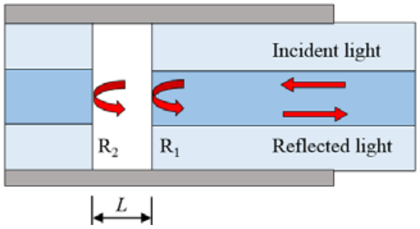


Figure 1. Illustration of a typical EFPI.

The phase difference between each reflected pair of the EFPI is given as:

$$\phi = \frac{2\pi}{\lambda} 2nL\cos(\theta) \tag{1}$$

When perturbation is introduced to the EFPI, the phase difference is influenced with the variation in the optical path length difference of the interferometer. Applying longitudinal strain to the EFPI sensor, for instance, changes the physical length of the cavity, which results in phase variation. By measuring the shift of the wavelength spectrum, the applied strain can be quantified.

EXPERIMENTAL PROGRAM

Test Specimens and Setup

Three S3×5.7 "I-shaped" steel beams were tested with a three-point bending setup in a compartment fire ('flame channel') as shown in Figure 2. Combined temperature and mechanical loading was applied. The three test beams were designated Beam #1, Beam #2, and Beam #3. Each of the beams had a 76 mm depth, 59 mm width, and 1420 mm length. The cross sectional area was 1077 mm^2.

A flame channel, which consisted of a burner rack, an enclosure, and a specimen loading system, was located under a 6 m × 6 m (plan) exhaust hood. The burner rack had four natural gas diffusion burners made of sheet metal, and each of the burners was 300 mm × 300 mm × 140 mm (length × width × height) in dimension. Natural gas entered a burner from the bottom, filled the burner cavity, and then, passed through a ceramic fiber blanket to distribute the gas. The burners were manually regulated by the energy content of the supplied gas, which was measured with an expanded uncertainty of less than 2.4 % [10]. An enclosure constructed of square tube steel, cold-formed steel C-profiles and gypsum board lined with thermal ceramic fiber enclosed the space above the burner rack. The enclosure was open at three faces: the bottom and the two ends in longitudinal direction of the beam, creating the compartment flame dynamics. The heated "compartment" created by the enclosure was approximately 380 mm × 400 mm × 1830 mm (height × width × length) in dimension. Each test beam was simply supported on two supports constructed of 1-1/2” Schedule 40 pipe, at a 1250 mm clear span. The specimen was loaded by a U-shape 1/2” Schedule 40 pipe (outer diameter: 21 mm) “loading yoke” at the mid-span. The supporting pipes and loading yoke were cooled with the exiting water temperature controlled to less than 50 °C. Load was transferred to the loading yoke with a pulley system.

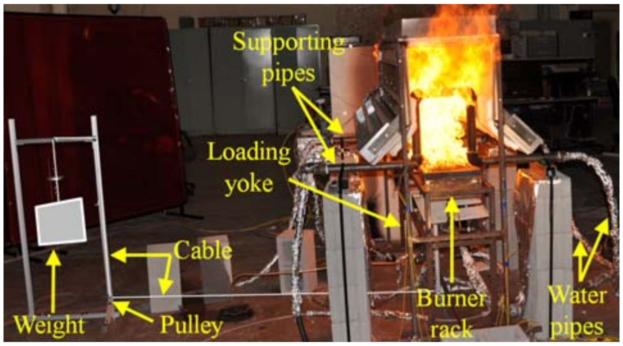


Figure 2. Experimental setup.

Instrumentation of Test Beams

Each beam was instrumented with four glass-sheathed, K-type, bare-bead thermocouples peened into small (diameter < 2 mm) holes, which were drilled into the bottom and top flanges as indicated in Figure 3: TC1 and TC3 at mid-span, and TC2 and TC4 at quarter-span. The thermocouples had a manufacturer-specified temperature standard limit of error of 2.2 °C or 0.75 % (whichever value is greater) over a measurement range of 0 °C to 1250 °C. A calibrated load transducer by Omegadyn was installed on a spanning bar at the bottom of the loading yoke and used to measure the applied load. The linearity and repeatability of the load transducer were ±0.03 % and ±0.01 %, respectively. Each beam was instrumented with one distributed fiber optic sensor (DFO-T) to measure temperature distributions, three distributed fiber optic sensors (DFO-ST1, DFO-ST2, and DFO-ST3) and three EFPI sensors (EFPI1, EFPI2, and EFPI3) to measure strains. The sensors EFPI1, EFPI2, and EFPI3 were closely deployed to DFO-ST1, DFO-ST2, and DFO-ST3, respectively.

Data from the fuel delivery system, thermocouples, displacement sensors and a load transducer were measured continuously using a National Instruments data acquisition system (NI PXIe-1082). Thermocouple data were recorded using 24-bit Thermocouple Input Modules (NI PXIe-4353), and load and displacement data were recorded using a high-speed, 16-bit multifunction module (NI PXIe-6363). Data were sampled at 90 Hz with average values and standard deviations recorded in the output file at a rate of 1 Hz.

A Neubrescope data acquisition system (NBX-7020) for the distributed fiber optic sensors was used to perform PPP-BOTDA measurements with 2 cm spatial resolution and accuracies of 0.75 °C and 15 με for temperature and strain, respectively. In this test, the spatial resolution was 2 cm, meaning that the Brillouin frequency shifts of two points spaced at no less than 2 cm could be distinguished. An optical spectrum analyzer (Yokogawa AQ6370C) was used to acquire data from the extrinsic Fabry-Perot interferometers with a broadband (1470 nm to 1630 nm) light source (Keysight 83437A). The operation wavelength ranged from 1500 nm to 1600 nm. The sampling frequency ranged from 0.2 Hz to 1 Hz.

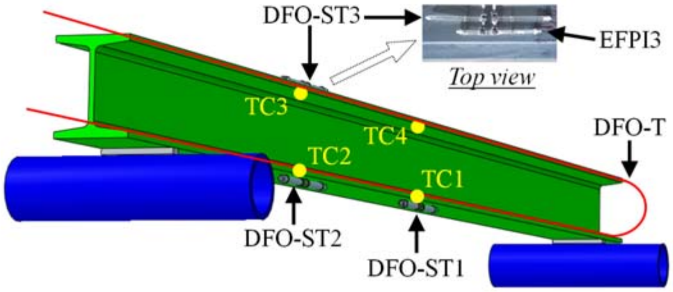


Figure 3. Instrumentation of test beams.

Test Protocol

Each beam was subjected to both fire and mechanical loading. Figure 4 illustrates the fire test protocol.

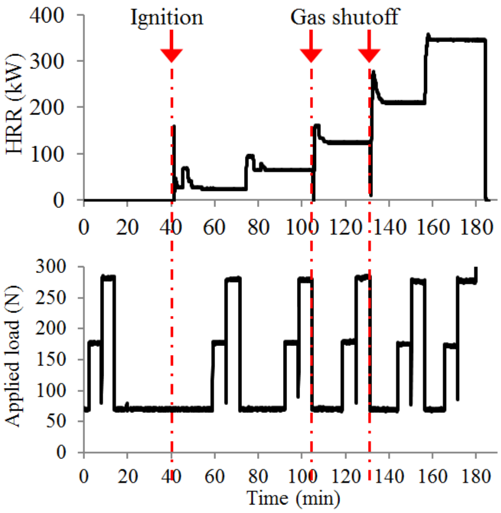


Figure 4. Test protocol.

The heat release rate (HRR) was held approximately constant at five target levels: 25 kW, 65 kW, 120 kW, 195 kW, and 350 kW, which corresponded to beam temperatures at TC1 of approximately 200 °C, 400 °C, 600 °C, 850 °C, and 1050 °C, respectively. During the test of Beam #2, the gas was turned off for about 20 seconds before the HRR was increased to 120 kW and 195 kW, respectively, to allow for visual observation. When the HRR was increased to a higher level, the target value was overshot and then quickly regulated down to the expected value. At each HRR level, in addition to the self-weight, the beam was subjected to three levels of loads at the mid-span. For Beam #1, the three loads were approximately 68 N, 98 N, and 126 N, and sustained for 7 minutes, 4 minutes, and 4 minutes, respectively. For Beams #2 and #3, the three loads were approximately 68 N, 176 N, and 285 N, each sustained for 6 minutes.

EXPERIMENTAL RESULTS AND DISCUSSION

Temperature Measurements

At each sustained HRR level, the beam temperature gradually stabilized to a temperature with some variation. To quantify the temperature variations, the mean values and standard deviations were calculated over 15 minutes for Beam #1, and 18 minutes for Beams #2 and #3 when the mechanical loads were applied at each temperature level. The coefficient of variation for all the thermocouple readings is less than 4 %. Similarly, to average out the effects of temperature fluctuation, five measurements were made using the DFO-T at each sustained temperature level. Each measurement was an implicit average over a time between 15 seconds and 40 seconds. The DFO-T readings have a maximum coefficient of variation of 4 %, which was similar to that of the thermocouples. The relative difference between the mean temperatures from the DFO-T and the thermocouple ranges from -10 % to 8 %. To understand the statistical significance of the measurement differences, the average of mean temperature differences (four for Beam #1, three for Beam #2, four for Beam #3) was calculated at each HRR level and presented in Figure 5 as an average temperature difference. In addition, the range of mean differences at 95 % confidence level is represented by the error bar.

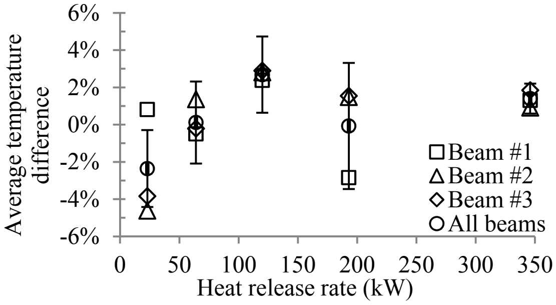


Figure 5. Difference between the fiber optic sensor and thermocouple temperature readings (error bars at 95% confidence).

It can be observed from Figure 5 that the mean difference at 95 % confidence level is less than 5 %, which is acceptable in many engineering applications. The discrepancies may be attributed to several factors. First, the DFO-T sensor was installed in a slightly different location than the thermocouples. Second, the thermocouple beads were located slightly below the surface of the beam and the DFO-T slightly above the surface, and thus, the influence of gas temperature variation on the measurements varied. Additionally, the thermocouples were not corrected for radiation losses.

Strain Measurements

The strain results measured from the EFPI sensors are plotted in Figure 6. As the HRR increases, the strain values approximately linearly increase. When the HRR was no more than 120 kW, the strain results from different sensors attached on different test beams agreed well. At the HRR equal to 120 kW, the strain values were approximately 8000 με to 9000 με. When the HRR became larger than 120 kW, greater variation of the strain results was observed from different sensors deployed at different locations. At the HRR equal to 350 kW, up to 35,300 με (3.53 %) strain was measured by the EFPI sensors.

Similar to the temperature measurements, multiple strain measurements were made from the distributed fiber optic sensors and EFPI sensors at each HRR level. The mean values for the two measurement methods were compared statistically for the conditions when the HRR was no larger than 120 kW, as shown in Figure 7. The mean strain difference at 95 % confidence level is less than 10 %. There are several reasons for the discrepancy between strain measurements from different sensors. First, the two sensors were deployed at slightly different locations that were subjected to different strains. Second, the data used to calculate the mean values of the two independent sensing systems were not selected at exactly the same moment. Although the two data acquisition systems were synchronized, they had different measurement (reading) durations, and thus, the measurement results were not achieved simultaneously. Third, each instrument has its own accuracy and repeatability at a level, and the measurement results contain error.

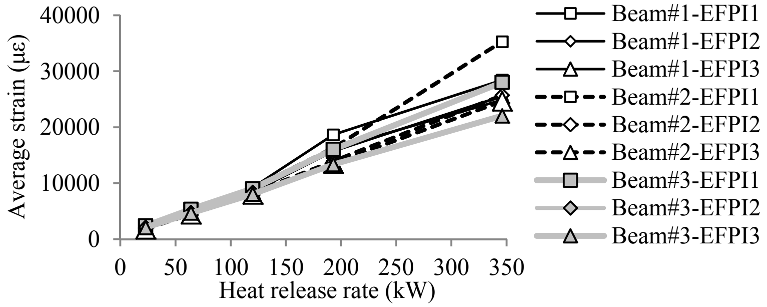


Figure 6. Average strain results measured from EFPI sensors.

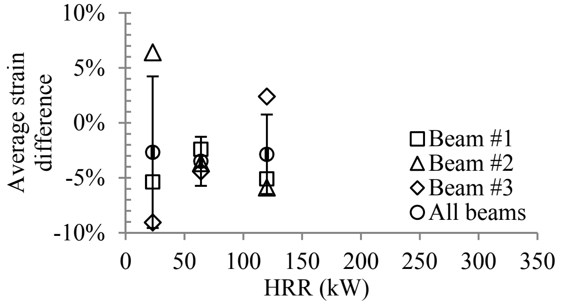


Figure 7. Difference between the distributed fiber optic sensor and EFPI sensor strain readings (error bars at 95% confidence).

CONCLUSIONS

Pulse pre-pump Brillouin Optical Time Domain Analysis distributed fiber optic temperature sensors have been demonstrated at temperatures up to 1050 °C in fire with adequate sensitivity and accuracy for typical structural engineering applications. These measurements add significant value over traditional thermocouples by providing distributed measurements over the length of the optical fiber with a spatial resolution of 2 cm. The measured temperatures were validated by thermocouples resulting in an average relative difference of less than 5 % at 95 % confidence level.

Extrinsic Fabry-Perot interferometric strain sensors have been demonstrated to operate up to 1050 °C in fire and measure at least 35,300 με (3.53 %) strains. The thermal strain predicted from the distributed fiber optic sensor and the extrinsic Farby-Perot interferometric sensor strain results were compared. The mean strain difference at 95 % confidence level was less than 10 %.

These results demonstrate the potential application of fiber optic temperature and strain sensors in structural fire testing. The investigated sensors provide increased temperature resistance, strain capacity, and spatial resolution when compared to traditional methods. Further development of the sensors is required to improve the robustness of the sensors and the speed of installation and measurement.

ACKNOWLEDGEMENT

This work was funded by the National Institute of Standards and Technology (NIST) under Award No. 70NANB13H183. The contents of this paper reflect the views of the authors, and do not necessarily reflect the official views or policies of NIST. Certain commercial equipment, instruments, or materials are identified in this paper to specify the experimental procedure. Such identification is not intended to imply recommendation or endorsement by NIST, nor to imply the materials or equipment are necessarily the best available for the purpose.

REFERENCES

1. Kodur, V., M. Dwaikat, and N. Raut. 2009. "Macroscopic FE model for tracing the fire response of reinforced concrete structures," Eng. Struct., 31 (10), 2368-2379.
2. Rinaudo, P., B. Torres, I. Paya-Zaforteza, P.A. Calderón, and S. Sales. 2015. "Evaluation of new regenerated fiber Bragg grating high-temperature sensors in an ISO834 fire test," Fire Safety J., 71, 332-339.
3. Bao, X., and L. Chen. 2011. "Recent progress in Brillouin scattering based fiber sensors." Sens., 11, 4152-4187.
4. Kishida, K., and C.H. Li. 2006. "Pulse pre-pump-BOTDA technology for new generation of distributed strain measuring system." Proc. Struct. Health Monit of Intel. Infrastruct., 471-477.
5. Bao, Y., and G. Chen. 2015. "Fully-distributed fiber optic sensor for strain measurement at high temperature." Proc. 10th Int. Workshop Struct. Health. Monit., Stanford, CA.
6. Rao, Y. J. 2006. "Recent progress in fiber-optic extrinsic Fabry-Perot interferometric sensors," Opt. Fiber Technol. 12, 227-237.
7. Bao, Y., W. Meng, Y. Chen, G. Chen, K.H. Khayat. 2015. "Measuring mortar shrinkage and cracking by pulse pre-pump Brillouin optical time domain analysis with a single optical fiber," Mater. Lett. 145, 344-346.
8. Bao Y, G Chen. 2016. "Strain distribution and crack detection in thin unbonded concrete pavement overlays with fully distributed fiber optic sensors." Opt. Eng. 55(1), 011008.
9. Bao, Y., and G. Chen. 2016. "Temperature-dependent strain and temperature sensitivities of fused silica single mode fiber sensors with pulse pre-pump Brillouin optical time domain analysis," Mes. Sci. Tech., under review.
10. Bundy, M., A. Hamins, E.L. Johnsson, S.C. Kim, G.H. Ko, and D.B. Lenhert. 2007. "Measurements of heat and combustion products in reduced-scale ventilation-limited compartment fires," NIST Technical Note 1483.

Enabling Quantitative Optical Imaging for In-die-capable Critical Dimension Targets

B.M. Barnes, M.-A. Henn, M. Y. Sohn, H. Zhou, and R. M. Silver,
National Institute of Standards and Technology, Engineering Physics Division,
100 Bureau Drive MS 8212, Gaithersburg, MD, USA 20899-8212

ABSTRACT

Dimensional scaling trends will eventually bring semiconductor critical dimensions (CDs) down to only a few atoms in width. New optical techniques are required to address the measurement and variability for these CDs using sufficiently small in-die metrology targets. Recently, Qin *et al.* [Light Sci Appl*,* 5, e16038 (2016)] demonstrated quantitative model-based measurements of finite sets of lines with features as small as 16 nm using 450 nm wavelength light. This paper uses simulation studies, augmented with experiments at 193 nm wavelength, to adapt and optimize the finite sets of features that work as in-die-capable metrology targets with minimal increases in parametric uncertainty. A finite element based solver for time-harmonic Maxwell's equations yields two- and three-dimensional simulations of the electromagnetic scattering for optimizing the design of such targets as functions of reduced line lengths, fewer number of lines, fewer focal positions, smaller critical dimensions, and shorter illumination wavelength. Metrology targets that exceeded performance requirements are as short as 3 μm for 193 nm light, feature as few as eight lines, and are extensible to sub-10 nm CDs. Target areas measured at 193 nm can be fifteen times smaller in area than current state-of-the-art scatterometry targets described in the literature. This new methodology is demonstrated to be a promising alternative for optical model-based in-die CD metrology.

Keywords: optical metrology, electromagnetic simulation, normalized sensitivities, parametric uncertainties, phase sensitive measurements, through-focus three-dimensional field

1. INTRODUCTION

Continuous advances in photolithographic technology, techniques, and materials have led to a downward scaling of the critical dimensions (CDs) of semiconductor devices. These CDs, often correlating to the line width of the features of interest, are presently below 20 nm and given current trends will likely reach the atomic scale in the mid-2020s [1]. Current metrology techniques are being refined to meet the challenges presented by such small features. For example, scanning electron microscopy (SEM) is being developed with multi-beam columns that allow the stitching of simultaneously acquired images over larger areas than presently possible for defect inspection [2] and may also be applicable to CD metrology. Also, modeling of the fundamental physics of electron scattering in materials is enabling new model-based measurements using SEM imaging for the metrology of CDs as small as 10 nm [3].

As these nascent advances are not yet fundamental to in-line process control in semiconductor manufacturing, the industrial workhorse for CD metrology remains optical scatterometry [4], as optics provides lower cost, greater areal coverage, and non-destructive measurements. Traditional placements of metrology targets for conventional scatterometry are illustrated schematically as Fig. 1. The measurement of the CD for features of interest is interpolated by evaluating the optical scattering from several multi-line arrays positioned on the scribe lines. From a manufacturing point-of-view, if the metrology is sufficiently accurate it is preferable to have metrology targets outside the active areas to allow for more devices in the active area with no constraints upon circuit design. Additional measurements by single-column scanning electron microscopes (SEMs) augment the optical CD metrology. These measurements may be combined through hybrid metrology to lower the parametric uncertainty for scatterometry [5-8].

However, there is a desire to shift towards accurate in-die metrology. In overlay metrology, meaning the alignment of one photolithography layer with a previous layer, intra-die variability is an increasing concern [9]. As CDs decrease, a lack of CD process control similar to that in overlay may exist between device features of interest and the metrology targets at the scribe lines. It is an ongoing question whether the placement of a scatterometry target within the active area is practical. It is a substantial obstacle to interpret the scattering once the incident beam size exceeds the area of the target.

*bmbarnes@nist.gov; phone 1 301 975-3947; fax 1 301 975-4299; http://go.usa.gov/36fTB

Metrology, Inspection, and Process Control for Microlithography XXX, edited by Martha I. Sanchez, Vladimir A. Ukrainstev
Proc. of SPIE Vol. 9778, 97780Y · © 2016 SPIE · CCC code: 0277-786X/16/$18 · doi: 10.1117/12.2221920

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

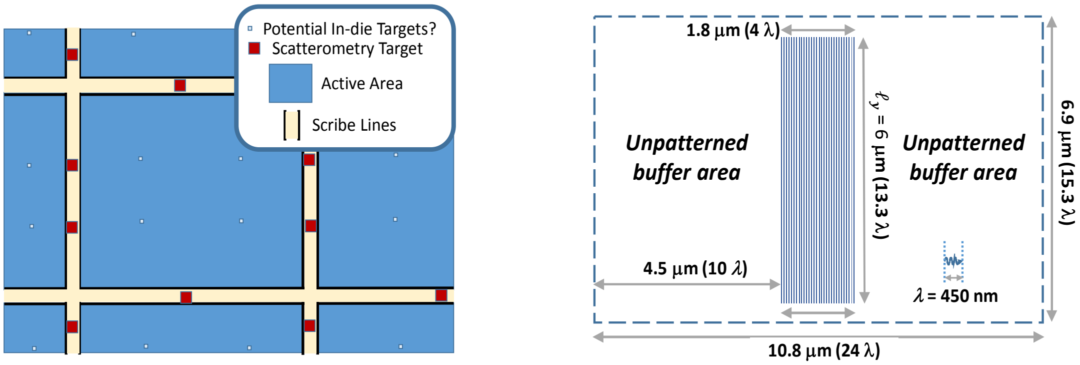


Figure 1. (left) Schematic (not to scale) of the traditional placement of critical dimension (CD) scatterometry targets relative to the active area in semiconductor manufacturing. The active area contains the billions of devices that constitute a successfully patterned computer chip. In current practice, interpolation of CD measurements on the scribe lines permits process control of CD within the active area. (right) Initial proposed in-die target design (to scale) based upon the measured target from Ref. [10]. The target has 30 lines with 60 nm pitch and line length (ℓ_y) of 6 µm. Two unpatterned buffer areas are to the left and right of the target to minimize optical interactions. Distances are shown in SI units and relative to the illumination wavelength from Ref. [10], λ = 450 nm. This paper explores through simulation optimizations of this target.

When the incident light underfills the target, the array can be often treated as a grating in simulation. When the beam overfills the target, "spurious" scattering and reflections arise that must be dealt with, although some metrology systems collect not only the 0th order-scattering but also the ±1st orders to augment their CD measurements [4]. Research is leading to reductions in the size of scatterometry targets, with some recent projections of targets as small as 12 µm x 12 µm in area for CD scatterometry [11] and 10 µm x 10 µm for diffraction-based overlay metrology [12].

In this present paper we suggest the industrial application of an alternative optical methodology that is not limited by the minimum spot size. The technique uses the broad continuum of scattered spatial frequencies that is inherent to a finite grating in order to parametrically determine the dimensions of a finite array of features. A recent paper [10] published by our group has demonstrated quantitative critical dimension measurements as small as 16 nm with parametric uncertainties as small as 1 nm or less. These finite arrays of features are of sufficiently small area to be considered for in-die metrology.

In Ref. [10], three 30-line arrays with deep-subwavelength dimensions were measured quantitatively. The narrowest of these lines was approximately 30 times smaller than the wavelength of the light, λ = 450 nm, used to measure them. Measurement was achieved by matching the scattered intensity profile against a library of simulated scattering profiles that were indexed by geometric parameters. Specifically, innovations in structured illumination [13], tool characterization and Fourier domain normalization [14], systematic error estimation, *a priori* information, and 3-D scattered light field analysis were all critical to unlocking deep-subwavelength information from sets of images acquired through-focus. This methodology is a new way of approaching the problem of in-die metrology and will have an impact upon how semiconductor manufacturers and equipment suppliers resolve critical issues in CD metrology.

Figure 1 shows schematically the potential placement of such in-die targets as well as a potential target design based upon the quantitative performance of the finite set of features in Ref. [10]. While the patterned area of the 30-line targets was 1.8 µm x 6 µm, for a realistic metrology target there must also be unpatterned regions in close proximity to serve as buffers to minimize optical interactions between the target and semiconductor devices of interest. Addition of these buffers increases the area of this initial proposed target at 450 nm wavelength to 10.8 µm x 6.9 µm, smaller than the 12 µm x 12 µm scatterometry targets for CD metrology in Ref. [11] above.

This paper uses simulation studies that are augmented with experimental data at λ = 193 nm to advance this methodology towards industrial relevance. The target design in Fig. 1 must be optimized for reduced area with sufficient accuracy. Also, experimental conditions (e.g., focus positions, wavelength) must also be optimized. In order to properly define the scope of these simulation studies, some review of the details of this technique from Ref. [10] are provided in Section 2 as well as information regarding the electromagnetic modeling. In Section 3, target and experimental parameters are defined and quantitative simulation study results are presented. These results are discussed further in Section 4 with respect to sensitivity, parametric correlation, and noise model. Sections 5 and 6 provide comparisons against conventional scatterometry and estimates of the extensibility of this optical imaging methodology, respectively. In Section 7, new experimental results at λ = 193 nm are shown to compare favorably to trends observed in the simulation study.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

2. SCATTERFIELD MICROSCOPY

2.1 Fundamentals of Scatterfield Microscopy

Scatterfield microscopy refers to the tailoring of the illumination and full use of the 3-D scattered light field above a scatterer to obtain metrology information [13,15]. Experimental methods for making full use of this light field have included angle-resolved imaging in a high-magnification platform [5,16-18] as well as the acquisition of focus-resolved images for defect metrology [16,19,20] and dimensional metrology [14,21].

The recently published work uses scatterfield microscopy to acquire images for the quantitative fitting of finite sets of features, which should be suitable as metrology targets, in a high magnification platform. There have been several key elements that were developed or refined to reach this objective. The process is described in full in Ref. [10] but summarized here for completeness. Quantitative measurement of these deep-subwavelength features is enabled by choosing a geometrical model from limited prior information, completing several electromagnetic simulations as functions of the parameters of that model, normalizing the simulated scattered fields using the observed tool functions, calculating images from those normalized fields, and estimating systematic errors including their correlations using nonlinear regression.

It is important to briefly compare the critical differences between the requirements of the experimental data fitting and these simulation studies. These studies assume a perfect microscope, negating the need for Fourier domain normalization of the scattered fields. In Ref. [10], it was determined that several of the systematic errors were correlated, increasing the complexity of the uncertainty analysis. In this work, the error model will be reduced to a simple, uncorrelated random error that is scaled to the incident intensity, I_0, as there is no systematic error or Type B uncertainty components to be considered in the perfect microscope. Therefore, the 1σ uncertainties (coverage factor k=1) shown may be well below what is experimentally achievable. In the previous work, measurements were performed using a low illumination numerical aperture (INA) of 0.13 and a high collection numerical aperture (CNA) of 0.95 while moving the sample through-focus. For all wavelengths in these simulation studies, the chosen INA is 0.1, except where noted. The electromagnetic modeling and nonlinear regression will be discussed in more detail below as they are essential to the simulation studies presented in this work.

2.2 Modeling of Scatterfield Microscopy

The software that has been used in most of the present study is the commercially available *JCMsuite**[22], a solver for time-harmonic Maxwell's equations and other applications using the finite element method (FEM). The FEM approach together with the use of perfectly matched layers as absorbing boundaries makes it possible to investigate the scattering from a variety of non-periodic 2-D and 3-D geometries. In Ref. [10], modeling was performed using an in-house implementation of the rigorous coupled-wave analysis (RCWA) with 2-D scattering and an assumption that the target was of sufficient length to be approximated as an infinite line, an assumption tested in the next sub-section.

Subsequent imaging of the scattering structures requires taking only the far field data into account. Here, the Fourier transform corresponding to the returning part of the total field is determined and the Fourier spectrum is used as input to propagate the field and calculate the images at different focus positions. In order to account for a finite INA we treat the light in the illumination path as the sum of plane waves originating from different points in a plane that is conjugate to the back focal plane (CBFP) of the objective lens. Here, a total of 12 plane waves are required to simulate this finite, 0.1 INA aperture, with each single plane wave taking about 70 s to calculate. Twelve plane waves have proven to be a good compromise between accuracy and computational effort; by taking advantage of the four-fold symmetry of the target geometry and the illumination set up, the finite aperture is computed with just three plane waves. Depending on the wavelength, the number of Fourier components lies around 520 per incident plane wave.

*Certain commercial materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials are necessarily the best available for the purpose.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

The images were calculated at 11 equally spaced focus positions relative to the substrate, for two orthogonal polarization states. As the depth of focus varies inversely with wavelength λ, to make the results comparable the maximum and minimum values of the focus positions $z_{min,max}$ were adjusted such that $|\frac{z_{min,max}}{\lambda}| = const$, leading to a range from -2 µm to 2 µm for $\lambda = 450$ nm and -0.86 µm to 0.86 µm for $\lambda = 193$ nm. The sampling rate in x direction corresponds to a pixel size of 25 nm with an overall range of 3 µm between -1.5 µm to 1.5 µm relative to the center of the structure. Together with the above specifications this configuration leads to an individual data set for each simulated intensity profile that consists of 2640 data points.

Cross-sectional views of the structures in the two geometry models used in these simulation studies are shown in Fig. 2. In the coordinate system shown at the far left of Fig. 2, the 2-D line and fin structures extend in the y direction, with infinite length for 2-D modeling and fixed widths in 3-D modeling, with the focus variation along the *z* direction.

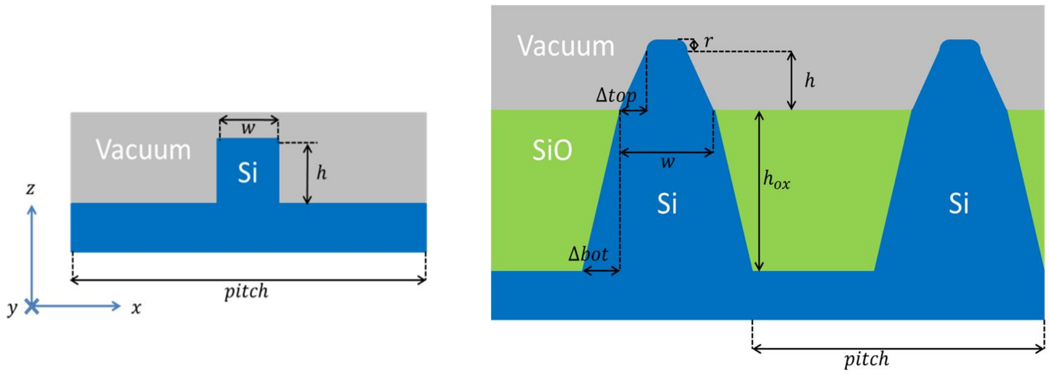


Figure 2. Cross-sectional views of single lines in the geometry models used in the simulation studies. The coordinate system is defined at the far left. (left) the "rectangular" model with floated parameters *w, h*. Single plane-wave illumination was used for this structure. (right) the "fins" model with floated parameters *w, h* with h_{ox} fixed.

Key considerations in choosing the geometric models for the simulation studies were parametric correlation and applicability to the semiconductor industry. The simplest possible model is a rectangular cross-section, and generally speaking the parametric correlation between the height and width parameters should be low in both cases. As this geometry is not reflective of actual manufacturing geometries, a second, more realistic, geometry model with fins and a SiO_2 layer was used. Again, in the interests of simplicity a single height and single width parameter were floated with the sidewall angle of the buried structure, the optical constants, and the SiO_2 oxide height all fixed. The number of geometric parameters and the optical properties of the materials involved can be expressed mathematically as the vector of parameters $\boldsymbol{a} = \{a_1, \dots, a_k\}$ with notation following Ref. [8].

2.3 Minimum Line Lengths

As a demonstration of the comparisons that are enabled by simulation studies on these structures, a qualitative study of the effects of finite line lengths, ℓ_y , upon the array is provided. Here, only a single plane wave of illumination was used for these comparisons. In Fig. 3, the scattering intensity profiles at two orthogonal polarizations and three focus heights are shown for 450 nm wavelength light incident upon an array of 10 rectangular lines. The varied parameter in this study is the length of the finite line array, i.e. the extension in z direction (cf. Fig. 2). Obviously there will always be a numerical difference between simulating finite isolated structures and simulations using 2-D codes, which implicitly assume infinitely long lines. One may still seek a minimum length $\ell_{y,\min}$ such that the modeling error incurred by using the 2-D code can be neglected within a chosen accuracy limit in order to optimize the tradeoff between accuracy and the computation time and resources relative to a full 3-D treatment.

At the left of Fig. 3, the differences are difficult to discern graphically between the finite and infinite scattering profiles imaged when the focus is at the substrate for lines at least 4000 nm in length. In the middle and right of Fig. 3, however, these distinctions for the finite line lengths are more apparent as the focus position increases. This is due primarily to an increase in the scattering interactions between the two ends of these finite lines that obscure the scattered intensity profile from the centers of the lines with increased defocus. It may be more useful to consider ℓ_y in determining the focal range

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

$z(\ell_y)_{\max}$ over which a finite length target can be used. Based on our understanding of the scattering of finite targets, for length $\ell_y = 6$ µm, the similarity between finite and the infinite model is sufficient for simulations of the rectangular structure for $z(\ell_y)_{\max} < 2$ µm, with a perceptible difference at ±2 µm, likely due to a minor resonance occurring due to single plane wave scattering.

A 6 µm line length is just over 13 wavelengths long at $\lambda = 450$ nm. The scattering interaction distance should decrease linearly with wavelength, implying that, for these simple targets, it should be possible to reduce line lengths to as short as short as 3 µm at 193 nm wavelength. Similarly, the 10 wavelengths-wide buffer areas should also lead to a decreased width. From wavelength scaling it should be possible to reduce the scatterfield microscopy target down to an area below 7 µm x 3 µm at λ = 193 nm, which if possible would represent a factor of fifteen less area than the 12 µm x 12 µm scatterometry target from Ref. [11].

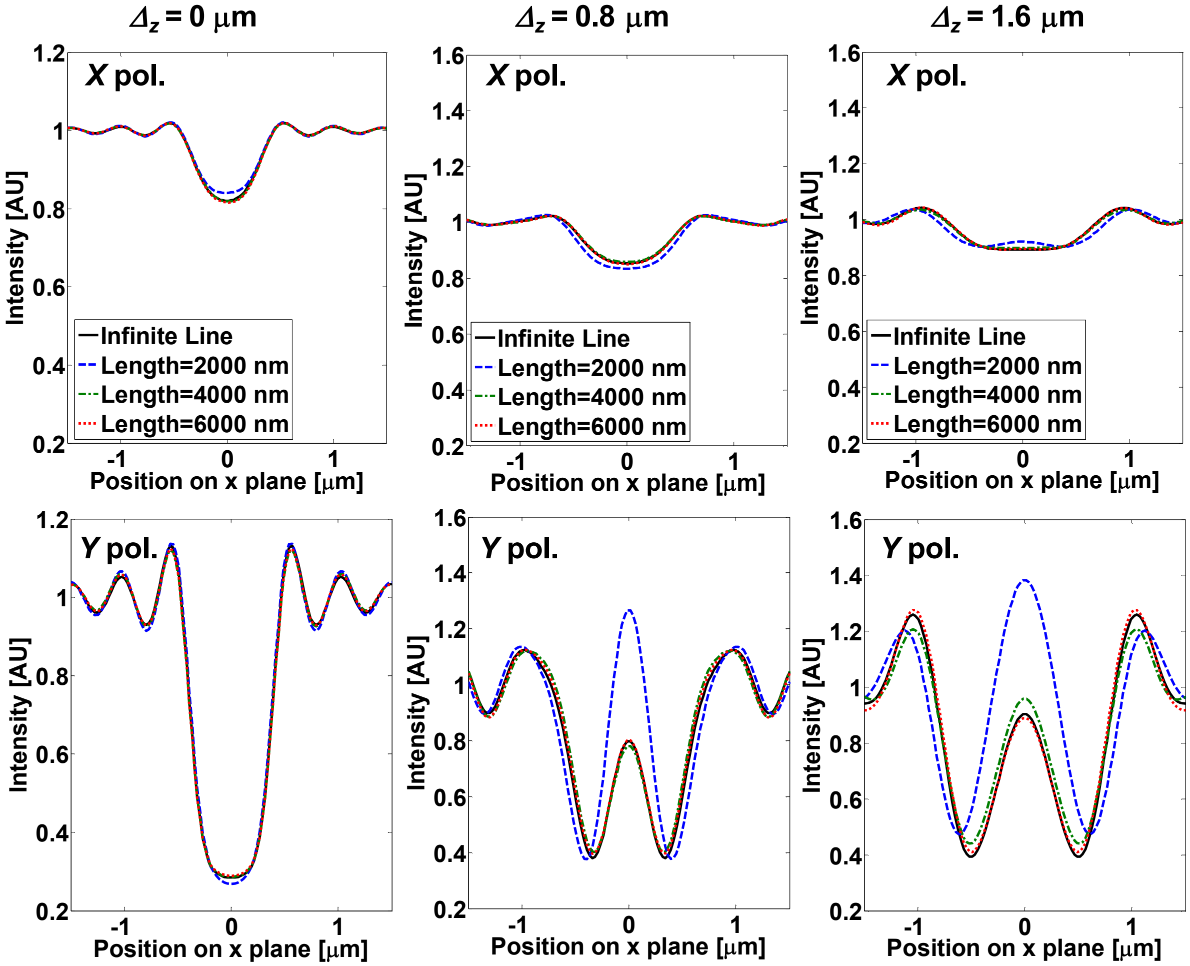


Figure 3. Simulated scattering intensity profiles at three focus positions for varying line lengths. *X, Y* polarizations are shown on the top and bottom, respectively, for $\lambda = 450$ nm illumination. The focus positions are relative to the substrate and are defined as $\Delta_z = 0$ µm at left, $\Delta_z = 0.8$ µm in the middle column, and $\Delta_z = 1.6$ µm for the left column. Qualitatively, there is little distinction between the infinitely long and 6000 nm long lines within this focal range, but further research is required to validate this trend.

3. SIMULATION STUDY RESULTS

Quantitative analyses of parametric uncertainties from simulation data are now used to study the capability of scatterfield microscopy to determine the geometrical parameters of the line/fin structures described above and more importantly,

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

address the question of what an optimized combination of target and experimental would be that would require the least area on the wafer while being sized large enough for an accurate determination of the critical dimensions (CD) using scatterfield microscopy. Since in the regime where $\lambda \gg CD$ metrology is only possible using a model-based approach, we will review some basic facts about regression, before investigating the effects of changes in the measurement setup and in the measured targets. The approach to these simulation studies can be generalized and is by no means tied to a particular instrument. Again, we will use the nomenclature as defined as provided in Ref. [8].

3.1 Regression of Simulated Data

In model-based metrology the parameters of interest, e.g., the height (h) and width (w) of a line structure, are determined by non-linear regression. Given a vector of measurement data $\{y_1, \dots, y_N\}$ and a physical model that yields simulation data $\{y(x_i, \boldsymbol{a})\}, i = 1, \dots, N$ that depend on the parameters of interest $\boldsymbol{a} = \{w, h\}$, we have a nonlinear regression for y_i and $y(x_i, \boldsymbol{a})$ given by

$$y_i = y(x_i, \boldsymbol{a}) + \epsilon_i, \tag{1}$$

with ϵ_i being the corresponding error on the i-th data point. We assume the random vector $\boldsymbol{\epsilon} = \{\epsilon_1, \dots, \epsilon_N\}$ to be Gaussian with zero mean and covariance matrix $\boldsymbol{V}$. Once the best fit value $\widehat{\boldsymbol{a}}$ is found, its uncertainty can be estimated using the covariance matrix

$$Cov[\widehat{\boldsymbol{a}}] = \left(\boldsymbol{D}(0)^T \cdot \boldsymbol{V}^{-1} \cdot \boldsymbol{D}(0)\right)^{-1}, \tag{2}$$

$$\text{with } \boldsymbol{D}(0) = \begin{bmatrix} \frac{\partial y(x_1,\boldsymbol{a})}{\partial a_1} & \cdots & \frac{\partial y(x_1,\boldsymbol{a})}{\partial a_k} \\ \vdots & \ddots & \vdots \\ \frac{\partial y(x_N,\boldsymbol{a})}{\partial a_1} & \cdots & \frac{\partial y(x_N,\boldsymbol{a})}{\partial a_k} \end{bmatrix}, \tag{3}$$

denoting the Jacobian matrix of the model function at the best fit value. In the context of regression this matrix is sometimes also called the sensitivity matrix, a term that will become clearer in Section 4. From Eq. (2) it can be seen that the uncertainty of the estimated parameters depends both on the variance of the input data and the simulations of the physical model.

The best fit value is usually found using gradient based optimization algorithms. Depending on the initial guess and the non-linearity of the model function this might be a cumbersome process, for each step requires the rigorous simulation of the scattering process. We therefore generate a grid on which we interpolate the model function, decreasing the computation time to 0.05 s for a single evaluation of the interpolation.

In order to prevent inverse crimes [23] we both generate the input data on a finer grid than the one we use for the regression and also add a 0.03 I_0 uncorrelated random background noise to it, hence $\boldsymbol{V} = (0.03)^2 \cdot \boldsymbol{I}_N$, with $\boldsymbol{I}_N$ denoting the N-dimensional identity matrix. This is in contrast to the full $\boldsymbol{V}$ matrix presented in Ref. [10] and is used to simplify the simulation study. Specifically, determining a new $\boldsymbol{V}$ matrix for every combination of wavelength, focus positions, and line number would be computationally prohibitive given the scope of this paper. Note that the 0.03 I_0 uncorrelated random background noise has different effects on the simulation data, since the reflectivity varies between the wavelengths and the structures, see Table 1 and Fig. 4.

Table 1. Reflectivity for the different structures as determined for the unpatterned buffer areas for two different wavelengths.

Reflectivity	$\boldsymbol{\lambda = 193\ nm}$	$\boldsymbol{\lambda = 450\ nm}$
Rectangles (Si)	0.67	0.42
Fins (SiO_2 layer on Si)	0.58	0.14

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

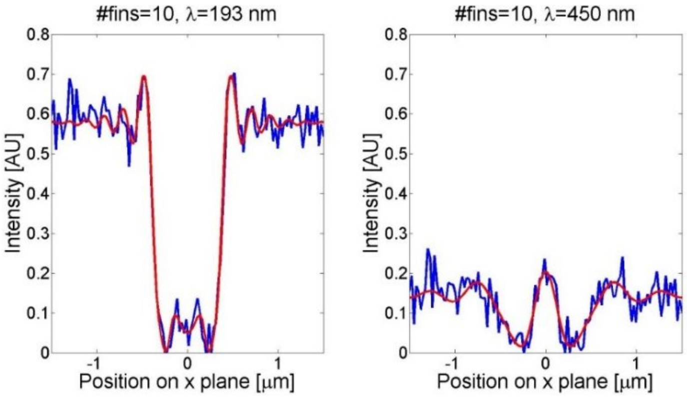


Figure 4. Simulated scattering intensity profiles for the 10 fins structure for two different wavelengths (left 193 nm, right 450 nm), unperturbed (red) and with added 0.03 I_0 random noise (blue).

3.2 Number of Lines Required

In this work we want to investigate how the parametric uncertainties change with respect to the structure itself. More precisely the total number of lines or fins is varied in this first simulation study. From an industrial point of view this directly addresses how large the target needs to be for metrological purposes. Several libraries were generated for increasing numbers of lines and fins, from 2 to 32 in steps of 2. The input data corresponds to a nominal line width of 20 nm and a height of 35 nm for the rectangular structure and a nominal line width of 25 nm and a height of 40 nm for the fins, with random background noise added in both cases. Again, we used a coarser grid for the regression, once the best fit values were found their uncertainties were estimated using Eq. (2).

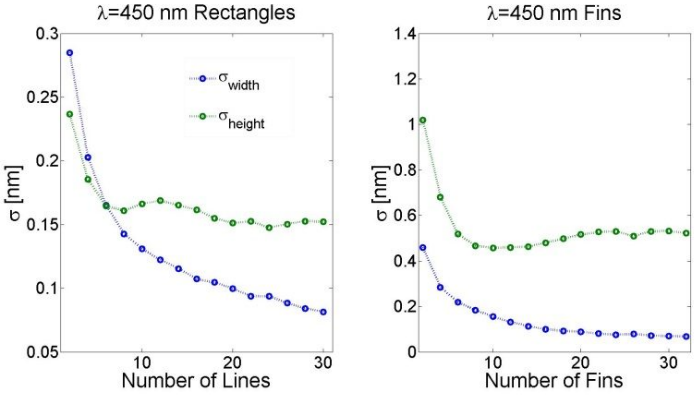


Figure 5. Dependence of the estimated uncertainties on the number of lines (left) and fins (right) of the investigated structure.

From the results, found in Fig. 5 above, one can see the target size can be reduced to 8 lines or 8 fins without losing too much accuracy on the determination of the height of the structure. There is some tradeoff regarding the uncertainty of the width, but the potential benefits from a decreased target size may outweigh the increased width uncertainty.

3.3 Number of Focus Positions Required

In the next step we want to investigate the dependence of the number of focus positions upon the parametric uncertainties. One of the 11 focus positions is randomly picked to start and successive focus positions are added, again randomly picked from the remaining ones, thus increasing the total number until having exhausted all 11 focus positions. In each step the

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

data sets are perturbed by adding random noise and used as input to the regression analysis. The resulting parametric uncertainties as a function of the number of focus positions are presented in Fig. 6.

Compared to using only a single focus height, uncertainties can be dramatically improved by adding as few as three or four focus positions. Of course the estimated uncertainties do not only depend on the number, but also on the actual focus positions selected, especially in the early stages of this process, when only one or two positions are considered. Since there are $\binom{n}{k}$ possibilities to choose k focus positions from a total of n available focus positions it is nearly impossible to determine the optimal order for all possible permutations. However, from the realizations that were investigated, these general trends with respect to the number of focus positions appear to hold independent of the order in which they are drawn.

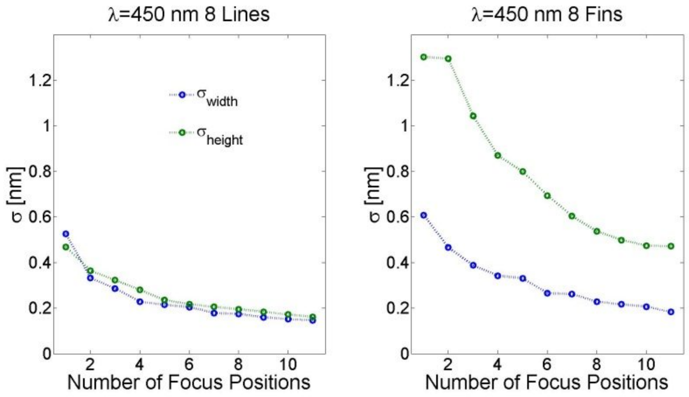


Figure 6. Dependence of the estimated uncertainties on the number of focus positions for rectangular profiles (left) and fins (right) using both polarizations for a single permutation of the focus positions.

Furthermore it was observed (not shown) that the uncertainties obtained using a wavelength of 193 nm in the simulations yields better results than using the larger wavelength of 450 nm. A detailed explanation for this behavior will be given in the upcoming section.

3.4 Dependence upon Illumination Wavelength & Incident Polarization

Finally, we want to present the estimated parametric uncertainties for a varying number of focus positions if only a single polarization is taken into account for the case of 8 fins and two wavelengths, 193 nm and 450 nm. An industrial measurement for example may select a single polarization to reduce measurement time. It turns out that for both wavelengths using only the *X* polarization data leads to very large parametric uncertainties. This is most problematic for the height parameter, which is therefore not shown here. The uncertainties for the width for both polarizations and the height for *Y* polarization for both wavelengths are presented in Fig. 7 below.

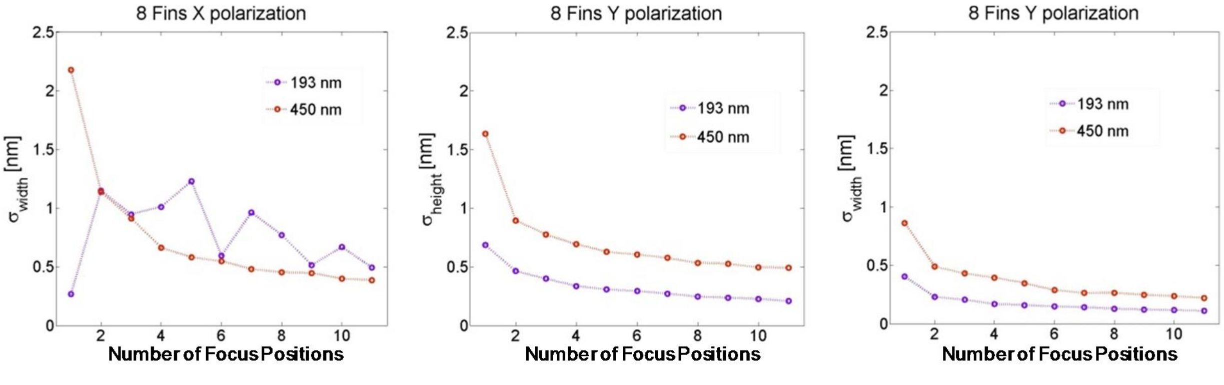


Figure 7. Dependence of the estimated uncertainties on the number of focus positions for 8 fins, taking only a single polarization into account.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

4. SENSITIVITY AND PARAMETRIC CORRELATION

Above, it has been shown that the target can be significantly smaller in area than that shown experimentally in Ref. [10]. Before accepting these findings at face value, the rationale behind these trends must be explored further to obtain a deeper understanding of the results presented above. A more detailed explanation of the results requires explanation of what governs the estimation of the parametric uncertainties. While the electromagnetic scattering from a finite set of features is an inherently non-linear problem, there are simple quantitative metrics that allow a qualitative understanding of the resultant parametric uncertainties. Many of the trends above can be explained by evaluating the sensitivity of the scattered intensity profiles and the parametric correlation inherent to the geometry and scattering. It has already been mentioned in the discussion of the regression approach that the parametric uncertainties depend on the Jacobian of the model function, also called the sensitivity matrix, and the covariance matrix of the error model. It is the interplay of those two quantities that eventually yields the parametric uncertainties in addition to the selected noise model. The noise model used on the scattered intensity profile in simulation studies provides the only source of error of the input data and for random error, scales the parametric uncertainty.

The first metric calculates the sensitivity of a specific tool producing a certain signal, with respect to a single measurand, e.g., the height or width of the profile. Here, this metric is a unitless, normalized sensitivity [24], defined as

$$normalized\ sensitivity = \frac{\Delta_{signal}/_{signal}}{\Delta_{measurand}/_{measurand}}. \tag{4}$$

It can be shown that for the simulations, the matrix consisting of the normalized sensitivities for all data points with respect to all measurands, i.e., model parameters, is proportional to the Jacobian, thus from Eq. (2) a high sensitivity leads to a small parametric uncertainty.

In addition, the quality of the reconstruction of the geometry parameters also depends on the ability of distinguishing if a change in the signal was due to a change in one or the other parameter. Therefore we additionally report a second metric, the parametric correlation, which can be found from calculating the correlation matrix $Corr[\hat{\boldsymbol{a}}]$ by

$$Corr[\hat{\boldsymbol{a}}] = \left(diag(Cov[\hat{\boldsymbol{a}}])\right)^{-1/2} \cdot Cov[\hat{\boldsymbol{a}}] \cdot \left(diag(Cov[\hat{\boldsymbol{a}}])\right)^{-1/2}. \tag{5}$$

Note that in the case of uncorrelated errors, i.e. a diagonal $\boldsymbol{V}$ matrix, both the normalized sensitivity and the correlation matrix only depend on the Jacobian matrix $\boldsymbol{D}(0)$ of the model function. Both the "fins" and "rectangular" geometries were parameterized with two floating parameters, and choosing only two parameters should lead to lower parametric correlations than models with three or more parameters, thus this simple case is a best-case scenario. However, if the parametric correlation is high for two parameters, the parametric correlation for more models with more variables should be much, much worse.

From Figs. 8 and 9, it can be shown how the normalized sensitivity and the correlation have an influence on the parametric uncertainties. Both figures are comprised of several parts. The top two rows in each Figure show the concatenation of 11 focus positions for two orthogonal polarizations. The dotted vertical lines separate out the 11 focus heights, while the two polarizations are color-coded, blue for *X* polarization and red for *Y* polarization. The normalized sensitivity within each dotted line is plotted as a function of position ranging from -2 μm to 2 μm on the unlabeled x axis of these two rows. The rows correspond to the normalized sensitivity with respect to the width and height, respectively. The matrix in the lower right of each Figure shows the absolute value of the correlation matrix, which by definition has unity on the diagonal, and it is the off-diagonal components that reveal parametric correlation. Finally, in the lower left of these figures, the parametric uncertainties are shown corresponding to that Figure.

The qualitative interpretation of these figures is more straightforward. Figure 8 corresponds to simulations of two fins at λ = 193 nm and shows an overall smaller normalized sensitivity and a larger parametric correlation with respect to Fig. 9, obtained from eight fins at λ = 193 nm. Comparing the two top rows in Fig. 8, it can be seen that the magnitudes of the

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

sensitivities scale with each other several data points, thus there is little to distinguish a change in height from a change in width. Therefore, there tends to be a higher parametric correlation between these two parameters in Fig. 8.

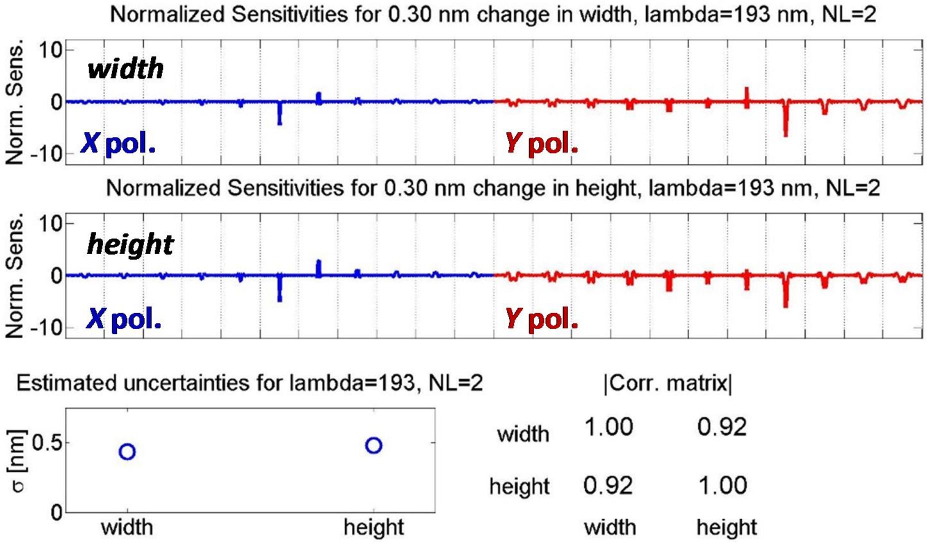


Figure 8. Normalized sensitivities and correlation matrices along with the resulting parametric uncertainties for a wavelength of 193 nm for two fins. The two top rows have unlabeled *x* axes due to the concatenation of the normalized sensitivity over 11 focus positions and two polarizations, denoted by dotted vertical lines. Within each of those 22 regions along the x axis, position -1.5 μm to 1.5 μm as shown in Fig. 4.

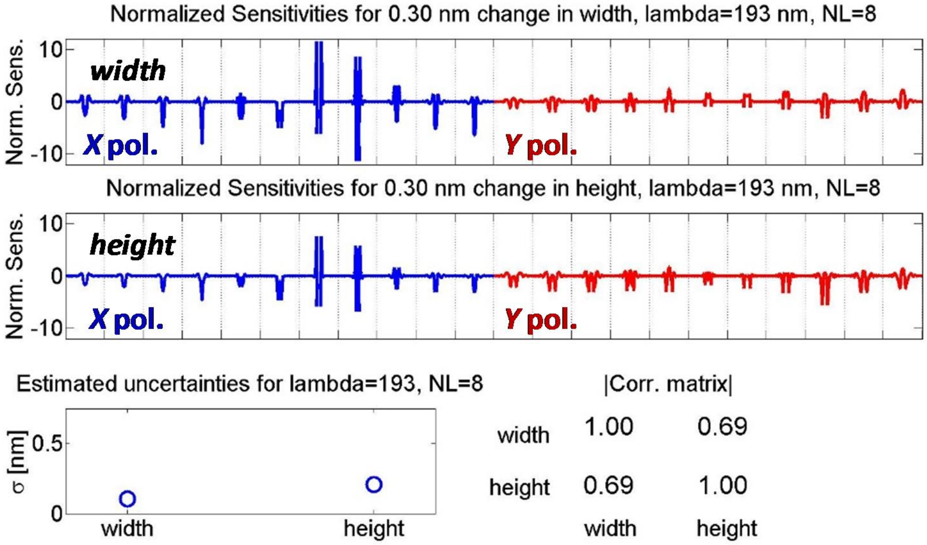


Figure 9. Normalized sensitivities and correlation matrices along with the resulting parametric uncertainties for a wavelength of 193 nm for eight fins. The two top rows have unlabeled *x* axes due to the concatenation of the normalized sensitivity over 11 focus positions and two polarizations, denoted by dotted vertical lines. Within each of those 22 regions along the *x* axis, position varies from -1.5 μm to 1.5 μm as shown in Fig. 4.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

It is therefore beneficial to choose an optimal combination of focus positions and number of lines or fins that lead to a very low uncertainty even for a small number of input data, as seen in Fig. 10 as a possible approach for industrial applications. There is no easy method for determining the optimal configuration given all the possible variations in the measurement setup and target geometries, yet examples such as Fig. 10 illustrate how tailoring the illumination, polarization, target design, and focus position may dramatically benefit the metrology community.

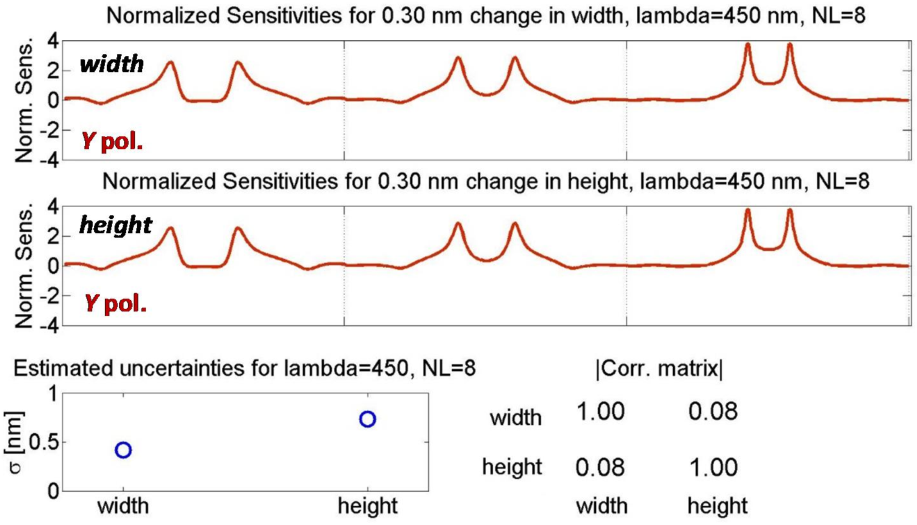


Figure 10. Normalized sensitivities and correlation matrices along with the resulting parametric uncertainties for a wavelength of 450 nm for eight fins and three focus positions and a single polarization (*Y*).

5. COMPARISON WITH CONVENTIONAL SCATTEROMETRY

While the potential benefits of reduced target size with respect to conventional scatterometry have been discussed, it is important to also compare simulated parametric uncertainties between conventional methods for scatterometry and this approach to scatterfield microscopy. Not all modes of scatterometry can be addressed in this paper, and the error model used in this analysis assumes the same error for both hypothetical tools (0.03 I_0) which may exceed the usual noise levels in scatterometry. However, as the parametric uncertainties scale linearly with this simple noise model, the comparison in this Section can serve as a key starting point for evaluating the merits of scatterfield microscopy to scatterometry.

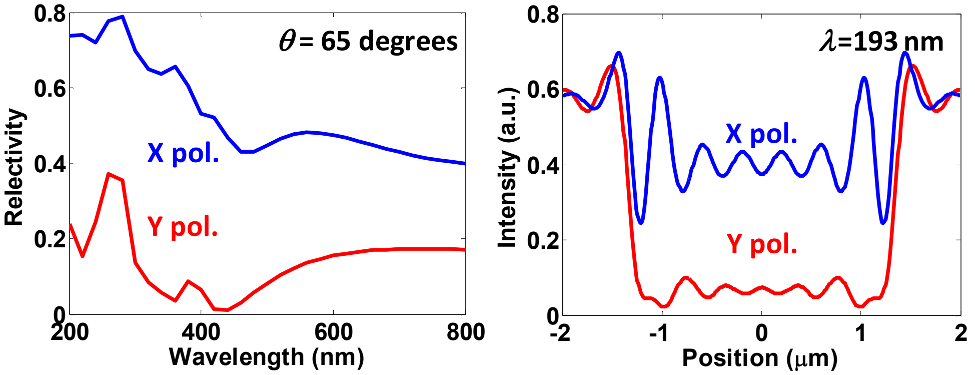


Figure 11. (left) Spectroscopic ellipsometry data. (right) Single-focus, scatterfield microscopy imaging with two orthogonal polarizations at λ=193 nm. The number of focus positions was greatly reduced in order to permit reduced data acquisition times in this simulation study.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

Using the RCWA model, simulations were performed for the 0th order scattering from a finite array of 30 fins to simulate spectroscopic ellipsometry [25] at a fixed incident angle of $\theta = 65°$. Shown as Fig 11, wavelengths were varied from 200 nm to 800 nm in 20 nm increments, and both the X and Y polarizations were calculated assuming single plane wave illumination. The spectroscopic ellipsometry yielded parametric uncertainties of σ_{width} = 0.50 nm and σ_{height} = 1.41 nm.

Scatterfield microscopy was simulated at λ = 193 nm for this same example using *JCMsuite* (not shown) for using 11 focus positions and 2 polarizations, yielding σ_{width} = 0.05 nm and σ_{height} = 0.15 nm. While this is dramatically less than the uncertainties for conventional scatterometry, the time required to acquire 11 images at two different polarizations may be impractical for in-line metrology. Therefore, for this comparison scatterfield microscopy has been limited to a single focus position and two polarizations as shown at the right of Fig. 11. The simulation with a single plane wave of illumination was performed in RCWA which requires periodic boundary conditions. To ensure minimal optical interactions between the periodic copies of the finite features, the period of the simulation domain was set to 10 µm, more than 22 wavelengths wide. Using these scattered intensity profiles, the parametric uncertainties increase to σ_{width} = 0.10 nm and σ_{height} = 0.34 nm. From this comparison, the two methodologies are comparable to each other.

6. COMPARISONS WITH EXPERIMENT

The simulation studies in this paper are designed to optimize the parametric uncertainties and minimize the area of the targets measured experimentally in Ref. [10]. To check the accuracy of the trends of these simulation studies, additional experiments are required. Here, three key targets are on the same wafer and in close proximity to the targets investigated in Ref. [10]. These new targets are measured at a shorter wavelength, λ = 193 nm. The first target is a 30-line target of nominally 16 nm width with 60 nm pitch and line lengths of 2 µm, which is three times shorter than the prior targets. This target will be used for qualitative evaluation of the effects of line length upon the scattered intensity profile. The second and third targets are 10-line targets of nominally 14 nm and 16 nm width with 60 nm pitch and 6 mm length. These targets demonstrate the sensitivity of the scattered intensity profiles to changes in line width. Each target was measured using scanning electron microscopy, from which widths were determined. For these targets, the nominally 14 nm and 16 nm wide, 6 µm long lines were on average (18.1 ± 0.9 nm) and (22.6 ± 1.1 nm) wide, respectively, while the nominally 16 nm lines of length 2 µm had a width of (22.8 ± 1.1 nm). These values are consistent with atomic force microscopy measurements on nearby targets as were presented in Ref. [10].

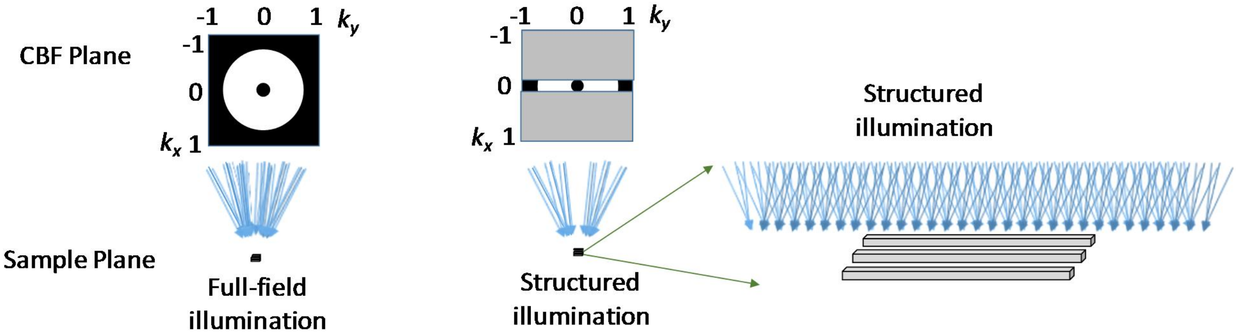


Figure 12. Comparison between typical full-field illumination and the structured illumination used in this experimental work. (left) Full-field illumination schematic, with accessible areas of the conjugate to the back focal plane (CBFP) shown in white. At the sample plane, a cone of illumination is incident on the sample. (middle) Structured illumination in the form of a slit in the CBFP. Far fewer angles of illumination are incident compared to the full-field. (right) Close-up of the sample. Placing the slit parallel to k_y puts the plane of incidence on average parallel to the lines, increasing sensitivity.

Experiments were performed using the NIST λ = 193 nm Microscope, a high-magnification imaging microscope that yields immediate benefits from wavelength scaling [26,27]. The system features a catadioptric objective lens with an inner CNA = 0.11 and an outer CNA=0.74, meaning that in full-field illumination the incident angles range from $\theta = 6°$ to $\theta = 48°$. The clear aperture in the CBFP for full-field illumination is shown at the upper left of Fig. 12. In this tool, on-axis illumination is not available, thus direct comparison with the simulation study is not possible. However, some benefits of a lower INA can be realized with sufficient illumination intensity by placing a slit aperture in the CBFP that is aligned parallel to the lines of the target. While the full range of k_y values are available to illuminate the target, the range of k_x values are dramatically decreased, meaning that no large angles of incidence are illuminating the target perpendicular to

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

the linear array, as shown in the middle of Fig. 12. The right of Fig. 12 shows that the structured illumination can be decomposed into several plane waves that, on average, are parallel to the direction of the length of the lines.

For each of the three targets, detailed focus-resolved images were collected. These data and their scattering intensity profiles are currently being processed for a sensitivity analysis and for quantitative imaging. Therefore, only a limited amount of the data can be presented in these Proceedings. However, the data shown and described here can provide a baseline for qualitative comparisons.

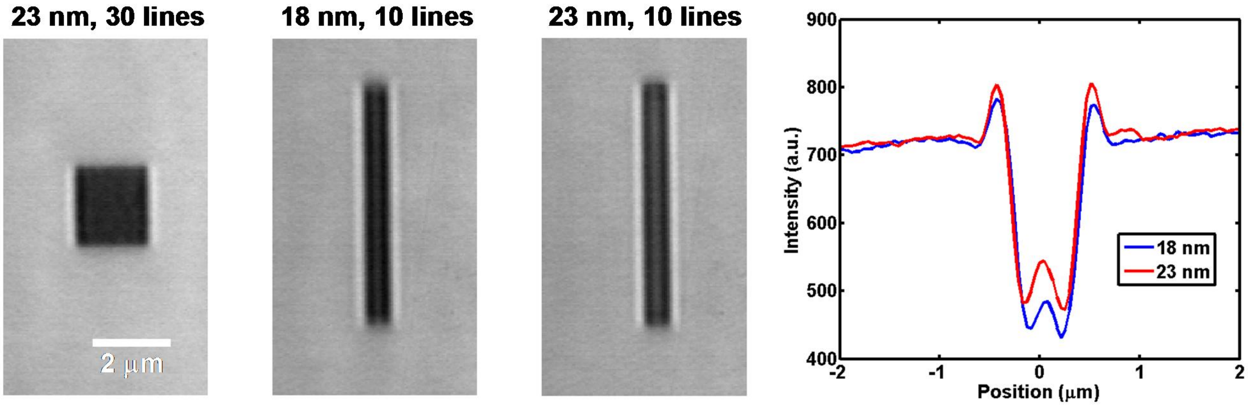


Figure 13. (left) Image of a 2 μm x 2 μm 30-line target with 18 nm or 23 nm wide lines running vertically. Scale bar applies to all images. (middle) Images of two 10-line targets of differing widths, each 6 μm long. Images are from nearly the same focal position. (right) Scattered intensity profile for the two targets shown in the middle.

The three targets are shown at focal positions where there is a strong constructive interference near the edges of the finite set of lines. However, it should be noted that the apparent “edge” signal is actually comprised of scattering from approximately 10 of the lines nearest that edge. For the 2 μm x 2 μm target at the left of Fig. 13, the scattered intensity profiles that could be taken from this image would be similar to each other throughout the middle 1.5 μm length of this target, indicating that the target could be further reduced in size in the vertical direction at this focal height. The scattered intensity profiles of the two targets in the middle are shown at the right of Fig. 13. A clear difference is seen in the profiles, indicating sensitivity.

Using Eq. 4, we can calculate the sensitivities for each position for the left image in Fig. 13 yielding a normalized sensitivity range for this target of -0.24 to 0.62. Further analysis of data from similar experiments indicates that the normalized sensitivities in general range from -0.5 to 0.5 and not -10 to 10 as in some of the simulation studies in Fig. 8. A primary reason for this discrepancy is likely the difference in different illumination and collection numerical apertures. Specifically, the simulation study assumed a narrower INA and a wider CNA. Subsequent simulation using the experimental INA and CNA has shown a reduction in the sensitivity to a range of approximately –3 to 2. Secondary reasons for any differences include noise in the experimental data and the implicit assumption is that all other target parameters are fixed while the width is increased in the experimental sensitivity study.

These experimental images and experimental normalized sensitivities are qualitative checks upon the quantitative values provided from the simulation study while confirming sensitivity to changes in width. This experimental sensitivity demonstrates that the picoscale uncertainties shown in some of the graphs likely underestimate the sensitivity and therefore the parametric uncertainties found through experiment may be higher than those reported in these simulation studies. However, the experimental data reinforces the potential impact of these in-die-capable targets.

7. EXTENSIBILITY OF SCATTERFIELD MICROSCOPY

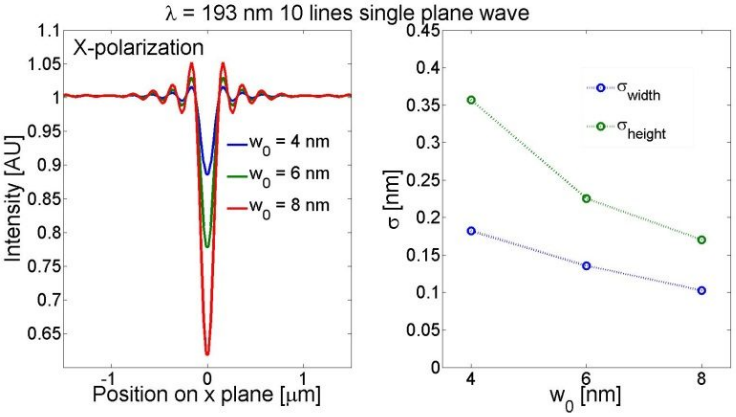
It must be further evaluated whether these targets are extensible to future semiconductor production nodes. Here, a simulation study is performed for 10 nm tall fins that range in width from 8 nm down to 4 nm. While it is known that

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

actual structures at sub-7 nm nodes may include concepts such as gate-all-around [28], this simple fin structure is preserved for easier comparison with the rest of this paper.

Simulations were performed using *JCMsuite* with single plane-wave illumination using two orthogonal polarizations at λ = 193 nm, imaging at 11 focus positions. This larger data set was used to establish the best case for extensibility. In Fig. 14 below, the quantitative performance of the imaging of 10 lines is shown for three different line widths. It can be directly observed that the signal for 8 nm CD is much stronger compared to 4 nm. Concatenation of all 11 focus positions and 2 polarizations (22 scanning intensity profiles) was used to calculate the uncertainties in the height and width parameters as shown at the right of Fig. 14. As expected, the parametric uncertainties increase as CD decreases. The proposed method appears extensible with current error model, multiple focus positions, and two polarizations.

Figure 14. Effects of decreasing widths upon CD measurements. (left) an image using *X* polarization at a single focus height. (right) Parametric uncertainties increasing with decreasing width.



It should be observed however that all model-based optical techniques, including scatterometry, must begin to incorporate the effects of quantum confinement as CDs shrink below 5 nm. Our group at NIST is illustrating possible effects upon the static dielectric constant as a function of nanowire diameters below 5 nm using the available literature, as is presented in the paper [29] in this Volume from Benjamin Bunday of SUNY Poly SEMATECH. We are preparing for the optical-based metrology of sub-5 nm features by presently tackling the fundamental physics of sub-5 nm low dimensional structures.

8. CONCLUSIONS

Based on a recently published paper [10] from our group that reported the quantitative measurement of deep-subwavelength, finite sets of features as small as 16 nm measured with λ = 450 nm light, this work presents simulation studies on the possibilities to extend this novel approach to different scatterometry targets and to a variety of tools with different inspection wavelengths. Additionally, we addressed the question of how to optimize the model-based measurement technique by investigating the effect of shorter line lengths, less lines, shorter wavelengths and smaller critical dimensions upon parametric uncertainties. It has been demonstrated that the methodology can be adopted with optimized targets by reducing the number of lines of the structure from 30 to 8 without sacrificing much of the method's accuracy, optimized data collection using a single polarization and reduced number of focus positions, and evaluated the maximum focal range for finite lines in terms of wavelength.

A deeper understanding of the underlying principles that govern the behavior of the parametric uncertainties was presented by taking into account the normalized sensitivity and the correlation between parameters. The data collected at an optimal choice of three focus positions and one polarization can be sufficient to yield a sub-nanometer parametric uncertainty. Providing an *a priori* algorithm to choose the optimal configuration however lies beyond the scope of this paper.

Nevertheless, it was demonstrated that even with four randomly picked, non-optimal, focus positions the results are very promising. Compared to conventional scatterometry, scatterfield microscope already yields smaller parametric uncertainties using a single focus height and two polarizations. Current estimates from simulation show the extensibility of the method to the measurement of structures as small as 4 nm.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

While some of the challenges that are present in a manufacturing environment, such as proper tool function characterization, have yet to be estimated, and future considerations such as the optical properties for CDs below 5 nm need to be explored further, the presented results show a promising route for model-based in-die metrology using a scatterfield imaging approach.

9. ACKNOWLEDGEMENTS

The authors thank Prem Kavuri and András Vladár of NIST for scanning electron microscopy measurements.

REFERENCES

[1] J. M. Shalf, and R. Leland, "Computing beyond Moore's Law," Computer 48(12), 14-23 (2015).

[2] A. L. Keller, D. Zeidler, and T. Kemen, "High throughput data acquisition with a multi-beam SEM." Proc. SPIE 9236, 92360B (2014).

[3] J. S. Villarrubia, A. E. Vladár, B. Ming *et al.*, "Scanning electron microscope measurement of width and shape of 10 nm patterned lines using a JMONSEL-modeled library," Ultramicroscopy 154, 15-28 (2015).

[4] J. d. B. Arie, "Optical wafer metrology sensors for process-robust CD and overlay control in semiconductor device manufacturing," Surface Topography: Metrology and Properties 4(2), 023001 (2016).

[5] R. M. Silver, B. M. Barnes, H. Zhou *et al.*, "Angle-resolved Optical Metrology using Multi-Technique Nested Uncertainties," Proc. SPIE 7390, 73900P (2009).

[6] N. Rana, and C. Archie, "Hybrid reference metrology exploiting patterning simulation," Proc. SPIE 7638, 76380W (2010).

[7] A. Vaid, B. B. Yan, Y. T. Jiang *et al.*, "Holistic metrology approach: hybrid metrology utilizing scatterometry, critical dimension-atomic force microscope and critical dimension-scanning electron microscope," Journal of Micro-Nanolithography MEMS and MOEMS 10(4), 043016 (2011).

[8] N. F. Zhang, R. M. Silver, H. Zhou *et al.*, "Improving optical measurement uncertainty with combined multitool metrology using a Bayesian approach," Applied Optics 51(25), 6196-6206 (2012).

[9] K. T. Turner, S. Veeraraghavan, and J. K. Sinha, "Relationship between localized wafer shape changes induced by residual stress and overlay errors," Journal of Micro/Nanolithography, MEMS, and MOEMS 11(1), 013001 (2012).

[10] J. Qin, R. M. Silver, B. M. Barnes *et al.*, "Deep subwavelength nanometric image reconstruction using Fourier domain optical normalization," Light Sci Appl 5, e16038 (2016).

[11] H. Cramer, S. Petra, B. O. Fagginger Auer *et al.*, "Intra-field patterning control using high-speed and small-target optical metrology of CD and focus." Proc. SPIE 9424, 94241F (2015).

[12] H.-J. H. Smilde, M. Jak, A. den Boef *et al.*, "Sub-nanometer in-die overlay metrology: measurement and simulation at the edge of finiteness." Proc. SPIE 8788, 87881N (2013).

[13] R. M. Silver, B. M. Barnes, R. Attota *et al.*, "Scatterfield microscopy for extending the limits of image-based optical metrology," Applied Optics 46(20), 4248-4257 (2007).

[14] J. Qin, R. M. Silver, B. M. Barnes *et al.*, "Fourier domain optical tool normalization for quantitative parametric image reconstruction," Applied Optics 52(26), 6512-6522 (2013).

[15] B. M. Barnes, R. Attota, R. Quintanilha *et al.*, "Characterizing a scatterfield optical platform for semiconductor metrology," Measurement Science and Technology 22(2), 024003 (2011).

[16] B. M. Barnes, F. Goasmat, M. Y. Sohn *et al.*, "Enhancing 9 nm Node Dense Patterned Defect Optical Inspection using Polarization, Angle, and Focus," Proc. SPIE 8681, 86810E (2013).

[17] R. M. Silver, B. M. Barnes, A. Heckert *et al.*, "Angle resolved optical metrology," Proc. SPIE*,* 6922 69221M (2008).

[18] B. M. Barnes, R. Attota, L. P. Howard *et al.*, "Zero-order and super-resolved imaging of arrayed nanoscale lines using scatterfield microscopy," AIP Conf. Proc. 931, 397-401 (2007).

[19] B. M. Barnes, F. Goasmat, M. Y. Sohn *et al.*, "Effects of wafer noise on the detection of 20-nm defects using optical volumetric inspection," Journal of Micro-Nanolithography MEMS and MOEMS 14(1), 014001 (2015).

[20] R. M. Silver, B. M. Barnes, Y. Sohn *et al.*, "The Limits and Extensibility of Optical Patterned Defect Inspection," Proc. SPIE 7638, 76380J (2010).

[21] R. M. Silver, J. Qin, B. M. Barnes *et al.*, "Phase sensitive parametric optical metrology: Exploring the limits of 3-dimensional optical metrology," Proc. SPIE 8324, 83240N (2012).

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

[22] S. Burger, L. Zschiedrich, J. Pomplun *et al.*, "JCMsuite: An Adaptive FEM Solver or Precise Simulations in Nano-Optics" in [Integrated Photonics and Nanophotonics Research and Applications], Optical Society of America, ITuE4, (2008).

[23] J. Kaipio, and E. Somersalo, [Statistical and computational inverse problems], Springer Science & Business Media, (2006).

[24] R. Silver, T. Germer, R. Attota *et al.*, "Fundamental limits of optical critical dimension metrology: a simulation study." Proc. SPIE 6518, 65180U (2007).

[25] J. Endres, A. Diener, M. Wurm *et al.*, "Investigations of the influence of common approximations in scatterometry for dimensional nanometrology," Measurement Science and Technology 25(4), 044004 (2014).

[26] M. Y. Sohn, B. M. Barnes, H. Zhou *et al.*, "Quantitative tool characterization of 193nm scatterfield microscope." Proc. SPIE 9556, 955611 (2015).

[27] Y. J. Sohn, R. Quintanilha, B. M. Barnes *et al.*, "193 nm angle-resolved scatterfield microscope for semiconductor metrology." Proc. SPIE 7405, 74050R (2009).

[28] C. P. Auth, and J. D. Plummer, "Scaling theory for cylindrical, fully-depleted, surrounding-gate MOSFET's," IEEE Electron Device Letters 18(2), 74-76 (1997).

[29] B. Bunday, "HVM metrology challenges toward the 5 nm node." Proc. SPIE 9778 (2016).

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 04/04/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

Quantum-Based Voltage Metrology with Superconducting Josephson Devices at NIST

S. P. Benz

National Institute of Standards and Technology, Boulder, Colorado, 80305, USA
Contact e-mail: benz@nist.gov

***Abstract* — Over the past three decades, the quantum behavior of Josephson junctions has been exploited to improve the accuracy of dc voltage measurements by five orders of magnitude. State-of-the-art precision voltage-standard systems based on arrays of superconductive Josephson junctions can now provide quantum-accurate, intrinsically stable, programmable voltages at amplitudes greater than 10 V for dc voltages and up to 2 V rms for synthesized ac voltages such as sine waves and arbitrary waveforms. Various measurement techniques have been developed for ac measurement applications in the audio-frequency regime and for 60 Hz power metrology. I describe the key developments in Josephson circuits and in measurement techniques, and summarize their current performance and limitations for voltage metrology applications. In particular, I emphasize how the use of quantum-based systems, even when they produce apparently low-uncertainty and reproducible results, does not guarantee that the measurements are accurate. Finally, I briefly summarize how quantum-accurate, arbitrary waveform synthesis is being used to measure Boltzmann's constant by measuring the Johnson noise of a resistor at the triple-point of water, and how a practical electronic primary temperature standard might be realized with a quantum-based Johnson noise thermometer.**

***Index Terms* — Digital-analog conversion, Josephson junction arrays, power measurement, precision measurements, signal synthesis, standards, superconducting integrated circuits, uncertainty, voltage measurement.**

Acknowledgment

The advancement of quantum-based voltage metrology has been and continues to be a world-wide research and development effort, including scientists, technologists, and metrologists. In particular, I thank and recognize all current and former members and guest researchers of the NIST Quantum Voltage Project and collaborators and colleagues from national and international measurement institutes and universities, all of whom have contributed to this field of research.

References

[1] J. Niemeyer, "Josephson voltage standards," in *Handbook of Applied Superconductivity*, vol. 2, B. Seeber, ed.,Institute of Physics, Philadelphia, PA, 1998, pp. 1813-34.

[2] C.A. Hamilton, "Josephson voltage standards", *Rev. Sci. Instrum.*, vol. 71, pp. 3611-3623, Oct. 2000.

[3] B. Jeanneret and S. P. Benz, "Application of the Josephson effect in electrical metrology," Proceedings of the International School on "Quantum Metrology and Fundamental Constants," Les Houches, France, 1-12 October 2007, eds. F. Piquemal and B. Jeckelmann, published jointly by EDP Sciences and Springer Verlag in The European Physical Journal Special Topics, vol. 172, 2009, pp. 181-206.

[4] S. P. Benz, "Synthesizing accurate voltages with superconducting quantum-based standards," *IEEE Instr. Meas. Magazine*, June 2010, pp. 8-13.

[5] S. P. Benz, "Quantum-based voltage waveform synthesis," in *100 Years of Superconductivity*, H. Rogalla and P. Kes, eds., Brussels: Chapman & Hall/CRC Press, 2011, pp. 546-552.

[6] A. Rüfenacht, L. Howe, A. E. Fox, R. E. Schwall, P. D. Dresselhaus, C. J. Burroughs, and S. P. Benz, "Cryocooled 10 V programmable Josephson voltage standard," *IEEE Trans. Inst. Meas.*, vol. 64, no. 6, pp. 1477-1482, June 2015, DOI: 10.1109/TIM.2014.2374697.

[7] N. E. Flowers-Jacobs, A. E. Fox, P. D. Dresselhaus, R. E. Schwall, and S. P. Benz, "Two-volt Josephson arbitrary waveform synthesizer using Wilkinson dividers," *IEEE Trans. Appl. Supercond.*, in press, DOI: 10.1109/TASC.2016.2532798.

[8] S. P. Benz, A. Pollarolo, Jifeng Qu, H. Rogalla, C. Urano, W. L. Tew, P. D. Dresselhaus, and D. R. White, "An electronic measurement of the Boltzmann constant," *Metrologia*, vol. 48, pp. 142-153, March 2011.

Contribution of NIST, not subject to copyright.

"Quantum-Based Voltage Metrology with Superconducting Josephson Devices at NIST."

Fast Dynamic Programming for Elastic Registration of Curves

Javier Bernal[1] Günay Doğan[1,2] Charles R. Hagwood[1]
[1] National Institute of Standards and Technology, [2] Theiss Research
{javier.bernal,gunay.dogan,charles.hagwood}@nist.gov

Abstract

Curve registration problems in data analysis and computer vision can often be reduced to the problem of matching two functions defined on an interval. Dynamic Programming (DP) is an effective approach to solve this problem. In this paper, we propose a DP algorithm that runs in $O(N)$ time to compute optimal diffeomorphisms for elastic registration of curves with N nodes. This algorithm contrasts favorably with other DP algorithms used for this problem: the commonly used algorithm of quadratic time complexity, and the algorithm that guarantees a globally optimal solution with $O(N^4)$ time complexity. Key to our computational efficiency is the savings achieved by reducing our search space, focusing on thin strips around graphs of estimates of optimal diffeomorphism. Estimates and strips are obtained with a multigrid approach: an optimal diffeomorphism obtained from a lower resolution grid using DP is progressively projected to ones of higher resolution until full resolution is attained. Additionally, our DP algorithm is designed so that it can handle nonuniformly discretized curves. This enables us to realize further savings in computations, since in the case of complicated curves requiring large numbers of nodes for a high-fidelity representation, we can distribute curve nodes adaptively, focusing nodes in parts of high variation. We demonstrate effectiveness of our DP algorithm on several registration problems in elastic shape analysis, and functional data analysis.

1. Introduction

Curve registration problems in data analysis and computer vision, e.g., horizontal alignment of chromatograms by domain warping, computation of elastic shape distances, can usually be reduced to the problem of matching two functions defined on an interval I in the real line. The problem of matching in turn usually involves computing an orientation-preserving diffeomorphism on the interval I to match each point in the range of one function with a point in the range of the other function, and vice versa. This is done by optimizing with respect to diffeomorphism, a data mismatch energy defined by data associated with the two functions. Dynamic Programming (DP) is widely recognized as an effective approach to solve such problems. However, although it computes globally optimal solutions, it is computationally expensive.

In the context of shape analysis, Srivastava et al. [1, 6, 9] proposed an algorithm for computing elastic shape distance between two closed curves in the plane using an $O(N^2)$ DP component for elastic registration of the curves, N the number of nodes per curve. It is computationally expensive as its total complexity is $O(N^3)$. A faster DP algorithm was proposed in [2] that works in a reduced search space (still $O(N^2)$ with a small constant), but computes very good diffeomorphisms. Note that a DP algorithm that would actually guarantee a globally optimal diffeomorphism by conducting a *complete* search would run in $O(N^4)$ time.

In what follows, we build on the works [5, 8], and describe computation in linear time of approximately optimal diffeomorphisms for elastic registration of curves. The diffeomorphisms are not guaranteed to be globally optimal, but we observed very convincing results in our experiments. Our DP approach uses concepts in [8], and similarly restricts its search to thin strips around graphs of estimates of optimal solution. It essentially uses a multigrid approach that projects, using DP, a diffeomorphism at a low resolution grid to one of higher resolution with this process continued recursively until a diffeomorphism of full resolution is obtained. This results in a fast $O(N)$ DP algorithm. We note, furthermore, that we implemented our algorithm to allow for curves of possibly unequal and nonuniform discretized domains of definition. In particular, our algorithm can be used for computing more efficiently elastic shape distances between closed curves in the plane with algorithms in [1, 9, 2, 3] by replacing their DP components with it. We present numerical results showing that our algorithm is much faster than the aforementioned DP components, and that with it, in particular, shape distance computation in [9] is indeed much faster while still producing distances as good as before. Finally, we present numerical results from using our algorithm for alignment of chromatograms in context of elastic functional data analysis.

Bernal, Javier; Dogan, Gunay; Hagwood, Robert.
"Fast Dynamic Programming for Elastic Registration of Curves."
Paper presented at the Proceedings of 2nd international workshop on differential geometry in
computer vision and machine learning (DIFF-CVML'16) in conjunction with CVPR 2016, Las Vegas, 2016., Las Vegas, NV, Jun 26-Jul 1, 2016.

2. Elastic Registration Formulation

For $F : [0, 1] \times [0, 1] \times \mathbb{R} \to \mathbb{R}$, we minimize energies of the following general form with respect to γ, γ a diffeomorphism of $[0, 1]$ onto itself with $\gamma(0) = 0, \gamma(1) = 1, \dot{\gamma} > 0$:

$$E(\gamma) = \int_0^1 F(t, \gamma(t), \dot{\gamma}(t))dt. \tag{1}$$

Many problems we find in applications of computer vision and scientific data analysis fall in the category of nonlinear data fitting, in which a target data function $y : \mathbb{R} \to \mathbb{R}^d$ is given, and the problem is then that of fitting or registering a model $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}^d$ to this data. This problem is often solved by optimizing (1) above with respect to γ for $F(t, \gamma(t), \dot{\gamma}(t)) = \|y(t) - f(\gamma(t), \dot{\gamma}(t))\|^p,\ p \geqslant 1$, a nonlinear regression problem. The elastic curve registration problems that we address in this paper fall in this category.

In practice, we need to solve a discretized version of the problem, either because the data itself is discrete, or due to the need to approximate the functions numerically. Thus, given a positve integer N, we choose a partition (not necessarily uniform) $\{t_l\}_{l=1}^N$ of $[0, 1]$, $t_1 = 0 < t_2 < \ldots < t_N = 1$, and discretize (1) with the trapezoidal rule:

$$E(\vec{\gamma}) = \frac{1}{2} \sum_{l=1}^{N-1} h_l (F(t_{l+1}, \gamma_{l+1}, \dot{\gamma}_{l+1}) + F(t_l, \gamma_l, \dot{\gamma}_l)), \tag{2}$$

where $\gamma_1 = 0, \gamma_N = 1$, $h_l = t_{l+1} - t_l$, $\gamma_l = \gamma(t_l)$, $\dot{\gamma}_l = (\gamma_{l+1} - \gamma_l)/h_l$, for $l = 1, \ldots, N-1$. We also add $\dot{\gamma}_N = \dot{\gamma}_1$ as a boundary condition for the derivative.

An important question then is the choice of discretization points $\{t_l\}_{l=1}^N$. This impacts both the efficiency and the accuracy of the solution. We propose an adaptive nonuniform discretization scheme that follows the complexity of the input data. In the case of a curve $\beta(t) : [0, 1] \to \mathbb{R}$ of curvature $\kappa(t)$, we can sample the curve to obtain nodes $\{\beta_l\}$, compute its discretized curvature $\{\kappa_l\}$ to measure geometric complexity, and choose discretization points accordingly. This motivates a two-step procedure

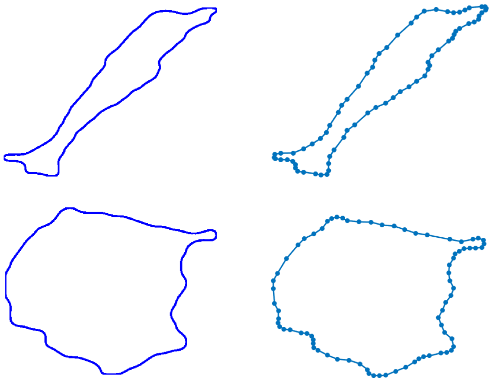


Figure 1. Adaptive nonuniform discretization of cell boundary curves. The curves on the left are high-fidelity uniformly sampled curves with $N = 1024$ nodes each. The curves on the right are adaptively sampled with $N = 74$ (top) and $N = 78$ (bottom) nodes, still maintaining a good representation of the geometry.

1. Distribute sample nodes $\{\beta_l\}$ such that pointwise geometric discretization error is below an acceptable tolerance: $\|\beta_l - \beta_{l-1}\|^2 \cdot \max(\kappa_l, \kappa_{l-1}) < 0.002$.
2. Compute lengths between consecutive nodes $\{\beta_l\}$, define arclength parameterization summing up lengths, and make discretization points associated with parametrization the choice of $\{t_l\}$.

Results of this procedure are illustrated in Figure 1.

3. Dynamic Programming (DP)

For positive integers N, M, not necessarily equal, and possibly nonuniform partitions of $[0, 1]$, $\{t_i\}_{i=1}^N$, $t_1 = 0 < t_2 < \ldots < t_N = 1$, $\{z_j\}_{j=1}^M$, $z_1 = 0 < z_2 < \ldots < z_M = 1$, we consider the $N \times M$ grid on the unit square with grid points labeled (i, j), i, j integers, $1 \leq i \leq N$, $1 \leq j \leq M$, each grid point (i, j) coinciding with planar point (t_i, z_j).

If the mesh of each partition, i.e., $\max(t_{m+1} - t_m), 1 \leq m \leq N-1$, and $\max(z_{m+1} - z_m), 1 \leq m \leq M-1$, is sufficiently small, then the set of diffeomorphisms γ of $[0, 1]$ onto itself with $\gamma(0) = 0, \gamma(1) = 1, \dot{\gamma} > 0$, can be approximated by the set of homeomorphisms of $[0, 1]$ onto itself whose graphs are piecewise linear paths from grid point $(1, 1)$ to grid point (N, M) with grid points as vertices. We refer to the latter set as Γ. Then γ in Γ is an approximate diffeomorphism of $[0, 1]$ onto itself and as such an energy conceptually faithful to (2) can be defined and computed for it. This is done one linear component of the graph of γ at a time.

Accordingly, given grid points (k, l), (i, j), $k < i, l < j$, that are endpoints of a linear component of the graph of γ, an energy of a trapezoidal nature over the line segment joining (k, l) and (i, j) is defined as follows:

$$E_{(k,l)}^{(i,j)} \equiv \frac{1}{2} \sum_{m=k}^{i-1} (t_{m+1} - t_m)(F_{m+1} + F_m), \tag{3}$$

$$F_m \equiv F(t_m, \alpha(t_m), L)), m = k, \ldots, i.$$

Here α is the linear function from $[t_k, t_i]$ onto $[z_l, z_j]$ whose graph is the line segment, $\alpha(t_k) = z_l$, $\alpha(t_i) = z_j$, and L is the slope of the line segment. Note $L = \frac{z_j - z_l}{t_i - t_k} > 0$ as $z_j > z_l, t_i > t_k$. The energy for γ is then defined as the sum of the energies over the linear components of the graph of γ with α in (3) coinciding with γ on each component.

For the purpose of efficiently computing γ^* in Γ of minimum energy, we present algorithm in next section that uses DP on grid points in strips around graphs of estimates of γ^*, one strip at a time. In this algorithm, a general DP procedure, Procedure *DP*, whose outline follows, is executed, for each strip, on set R of grid points inside strip. For such sets computational cost is low (search space is relatively small), and their selection is such that it is highly likely final DP solution is γ^* itself or at least close to it. Since the collection of such strips has the appearance of one single strip whose shape evolves as it mimics the shapes of graphs of estimates of γ^*, we think of the collection as indeed being one single strip, a dynamic strip that we call *adapting* strip accordingly. In [2], Dogan, Bernal and Hagwood proposed using a strip R of linear ($O(N)$) width around the diagonal of $[0, 1]^2$ connecting planar points $(0, 0)$ and $(1, 1)$, for a fast DP algorithm. In this work, rather than rigidly fixing R, we propose using an adapting strip as described above with a width that is constant ($O(1)$) as it evolves around graphs of estimates of γ^*. Obviously we do not know γ^*, but can estimate it using DP solutions on coarser grids. However, before going into the specifics of our proposed algorithm, we will describe Procedure *DP* operating on generic R.

The set R of labeled grid points can be any subset of the interior grid points plus the corner grid points $(1, 1)$, (N, M). Given any such R, we denote by $\Gamma(R)$ the set of elements of Γ with all vertices in R. Accordingly, with the energy in (3) adjusted for R (see below), given positive integer $layrs$ (e.g., $layrs = 5$) which determines the size of certain neighborhoods to be searched (see below), then, based on DP, Procedure *DP* that follows, in $O(|R|)$ time, will often (depending on $layrs$) compute optimal γ^* in $\Gamma(R)$, $|R|$ the cardinality of R.

As the DP procedure progresses over the indices (i, j) in R, it examines function values on indices (k, l) in a trailing neighborhood $N(i, j)$ of (i, j) (see Figure 2 for a particular R described below). In the full DP, we would be examining all (k, l) in R, $1 \leqslant k < i, 1 \leqslant l < j$. This has high computational cost, and is not necessary for our applications. Using a much smaller square neighborhood $N(i, j)$ of ω points ($\omega = layrs$) per side gives satisfactory results. Thus, for each (i, j) in R, we examine at most ω^2 indices (k, l) in the trailing neighborhood $N(i, j)$. Then the overall time complexity is $O(\omega^2|R|)$. We formally define $N(i, j)$ by

$$N(i,j) = \{(k,l) \in R : k \text{ is one of } \omega \text{ largest indices } < i \\ \text{and } l \text{ is one of } \omega \text{ largest indices } < j\}.$$

Note that in the unusual case $N(i, j)$ happens to be empty then a grid point (k, l) in R, $k < i$, $l < j$, perhaps $(k, l) = (1, 1)$, is identified and $N(i, j)$ is set to $\{(k, l)\}$

The DP procedure follows. First, however, we clarify some implicit conventions in the procedure logic. The main loop in the DP procedure takes place over the single index i (not the grid point (i, j)). We process index i in increasing order of its values, and for each value, each occurrence of the value is processed before moving to the next one. Also in the procedure, pairs of indices m_1, m_2 are retrieved from an index set $\mathcal{M}$, satisfying $m_1 < m_2$ with no other index in $\mathcal{M}$ greater than m_1 and less than m_2.

```
procedure DP
  $E(1,1) = 0$
  for each $(i,j) \neq (1,1)$ in $R$ in increasing order of $i$ do
    for each $(k,l) \in N(i,j)$ do
      $\alpha$ = linear function, $\alpha(t_k) = z_l$, $\alpha(t_i) = z_j$
      $L$ = slope of line segment $\overline{(k,l)(i,j)}$
      $\mathcal{M} = \{m : k \leq m \leq i, \exists(m,n) \in R\}$
      $F_m = F(t_m, \alpha(t_m), L)$ for each $m \in \mathcal{M}$
      $E^{(i,j)}_{(k,l)} = \frac{1}{2}\sum_{m_1,m_2\in\mathcal{M}}(t_{m_2} - t_{m_1})(F_{m_2} + F_{m_1})$
    end for
    $E(i,j) = \min_{(k,l)\in N(i,j)}(E(k,l) + E^{(i,j)}_{(k,l)})$
    $P(i,j) = \arg\min_{(k,l)\in N(i,j)}(E(k,l) + E^{(i,j)}_{(k,l)})$
  end for
end procedure
```

The optimal solution γ^* in $\Gamma(R)$ can then be obtained by backtracking from (N, M) to $(1, 1)$ with pointer P above. Accordingly, Procedure *opt-diffeom* that follows, will produce γ^* in the form $\vec{\gamma}^* = (\gamma^*_m)^N_{m=1} = (\gamma^*(t_m))^N_{m=1}$:

```
procedure opt-diffeom
  $\gamma^*_N = 1$
  $(i,j) = (N,M)$
  while $(i,j) \neq (1,1)$ do
    $(k,l) = P(i,j)$
    $\gamma^*_k = z_l$
    for each integer $m, k < m < i$ do
      $\gamma^*_m = \frac{(t_i - t_m)}{(t_i - t_k)} z_l + \frac{(t_m - t_k)}{(t_i - t_k)} z_j$
    end
    $(i,j) = (k,l)$
  end while
end procedure
```

The original $O(N^2)$ DP algorithm, which we call *original-DP*, was used in [1, 6] to compute elastic shape distances. It is essentially the same as Procedure *DP* above (for the proper instance of (2)) followed by Procedure *opt-diffeom*, using a uniform grid, $N = M$, and R equal to all interior grid points plus the corner grid points $(1, 1)$, (N, M). Depending on $layrs$, it computes optimal γ^* in Γ. In [2], a cheaper but still $O(N^2)$ version of *original-DP* called *fast-DP*, based on the Sakoe-Chiba Band [7], was presented for the same purpose. It is essentially *original-DP* with R equal to the corner grid points $(1, 1)$, (N, M) plus interior grid points inside a strip S of width d along the diagonal of unit square from $(0, 0)$ to $(1, 1)$ (see Figure 2). Depending on $layers$ and d, it computes optimal γ^* in Γ.

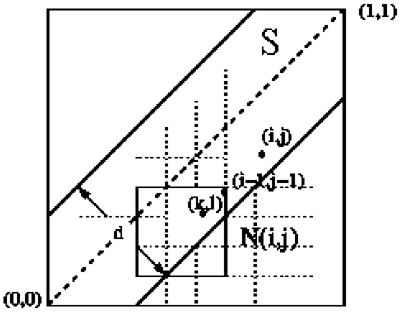


Figure 2. In *fast-DP*, R is set of interior grid points in strip S together with grid points at planar points $(0,0)$, $(1,1)$, i.e., $(1,1)$, (N,M). Given (i,j) in R, $i,j > 1$, then $N(i,j)$ in Procedure *DP* is the set of grid points in R on or inside the smaller square (here covering a 4×4 subgrid for $layrs = 4$) with right upper vertex $(i-1,j-1)$. Only the grid points in $N(i,j)$ are considered in Procedure *DP* for the left lower endpoint of line segment ending at (i,j) that makes $E(i,j)$ in Procedure *DP* the smallest.

4. Dynamic Programming Restricted to an Adapting Strip

The *DP* algorithms *original-DP* and *fast-DP* used in [1, 9, 2, 3] are essentially the same as Procedure *DP* (for the proper instance of (2)), using a uniform grid, $N = M$, and particular sets of grid points for R. Clearly, under these conditions, the possibility is then precluded of using either one of them for elastic registration of curves whose defining point sets have been either refined or coarsened due, for example, to curvature considerations.

In what follows, working with partitions (not necessarily uniform) of $[0,1]$, $\{t_l\}_{l=1}^{N}$, $\{z_l\}_{l=1}^{M}$, as previously described, we present a linear algorithm which we call *adapt-DP*, based on DP restricted to an adapting strip, to compute optimal diffeomorphisms for elastic registration of curves. It has parameters $layrs$, $lstrp$, set to small positive integers, say 5, 30, respectively. Parameter $layrs$ is as previously described, while $lstrp$ is an additional parameter that determines width of adapting strip (see below). Although *adapt-DP* is not guaranteed to be always successful, it has been observed to produce convincing results in our experiments. The original ideas for this algorithm are described in [5, 8] in the context of graph bisection and dynamic time warping.

As presented below, for a given instance of (2)), *adapt-DP* is essentially an iterative process that restricts its search to the adapting strip around graphs of estimated solutions. Each iteration culminates with execution of Procedure *DP* for recursively projecting a diffeomorphism obtained from a lower resolution grid to one of higher resolution until full resolution is attained. For simplicity, we assume here $N = M = 2^n + 1$ for some positive integer n. Extension of the algorithm to allow N, M to have any values is straightforward. Note we don't assume partitions $\{t_l\}$, $\{z_l\}$ are uniform. Finally, after last execution of Procedure *DP* in *adapt-DP*, Procedure *opt-diffeom* is performed to obtain, depending on $layrs$ and $lstrp$, optimal γ^* in Γ. Algorithm *adapt-DP* follows:

```
algorithm adapt-DP
2. $I(1) = J(1) = 1$
3. $P(N,M) = (1,1)$
   for $r = 1$ to $n$ do
5.    $NI = NJ = 2^r + 1$
6.    for $m = 1$ to $NI - 1$ do
7.       $I(m+1) = m \cdot 2^{n-r} + 1$
8.       $r'_m = \frac{1}{2}(t_{I(m)} + t_{I(m+1)})$
      end for
      for $m = 1$ to $NJ - 1$ do
         $J(m+1) = m \cdot 2^{n-r} + 1$
12.      $s'_m = \frac{1}{2}(z_{J(m)} + z_{J(m+1)})$
      end for
14.   $r'_1 = s'_1 = 0$
15.   $r'_{NI-1} = s'_{NJ-1} = 1$
      $(i,j) = (N,M)$
      $D = \emptyset$
18.   while $(i,j) \neq (1,1)$ do
         $(k,l) = P(i,j)$
*********************************************
20. Here below, for integers $m'$, $n'$, $1 < m' < NI$,
21. $1 < n' < NJ$, bin $B(m',n') \equiv$
22. $\{(x,y) : r'_{m'-1} \leq x \leq r'_{m'}, s'_{n'-1} \leq y \leq s'_{n'}\}$
*********************************************
         identify bins $B(m',n')$, $1 < m' < NI$,
         $1 < n' < NJ$, the interiors of which are
         intersected by line segment $\overline{(i,j)(k,l)}$
         $D' = \{(m',n') : \overline{(i,j)(k,l)} \cap B(m',n') \neq \emptyset\}$
         $D = D \cup D'$
         $(i,j) = (k,l)$
      end while
      $R = \{(1,1),(N,M)\}$
31.   for each $(m',n')$ in $D$ do
         $i_0 = \max\{2, m' - lstrp\}$
         $j_0 = \max\{2, n' - lstrp\}$
         $R_1 = \{(i,j) : i = I(i'), i_0 \leq i' \leq m', j = J(n')\}$
         $R_2 = \{(i,j) : j = J(j'), j_0 \leq j' \leq n', i = I(m')\}$
         $R = R \cup R_1 \cup R_2$
      end for
38.   execute procedure DP on $R$
   end for
   execute procedure opt-diffeom to obtain $\gamma^*$
end algorithm
```

In outline of *adapt-DP* above, we note in line 5, NI starts equal to 3 (for $r = 1$) and then it is essentially doubled at each iteration $r > 1$ until it becomes equal to N at the n^{th} iteration. We note in line 2 and in line 7 inside **for** loop at line 6, range of I starts with 3 integers (for $r = 1$)

and then essentially doubles in size at each iteration $r > 1$, contains previous range of I from preceding iteration, and is evenly spread in the set $\{1, 2, \ldots, N\}$ until it becomes this set. We note as well from the well-known sum of a geometric series that since $N = 2^n + 1$ then the sum of the NI's, i.e., $(2^1 + 1) + (2^2 + 1) + \ldots + (2^n + 1)$, is $O(N)$. Clearly, all of the above applies to NJ, M, and range of J.

We note **while** loop at line 18 identifies certain cells in the Voronoi diagram [11] of the set of grid points $R' \equiv \{(i, j) : i = I(m'), j = J(n'), 1 < m' < NI, 1 < n' < NJ\}$ restricted to the unit square. Indeed bin $B(m', n')$ as defined in lines 20-22, in terms of the computations in lines 8, 12, 14, 15, is exactly the Voronoi cell of $(I(m'), J(n'))$, and all such cells together partition the unit square. Accordingly, with γ^* encoded in P in line 3 ($r = 1$) or in line 38 ($r > 1$) through the execution of Procedure *DP* in the previous iteration ($r - 1$), it must be that every point in the graph of γ^* is in some bin $B(m', n')$. Thus, it then seems reasonable to say that a reliable region of influence of γ^* is the region around the graph of γ^* formed by the union of bins within a constant number of bins from the graph. Accordingly, to be precise, a bin B is part of this region if and only if there is a bin B', the interior of which the graph of γ^* intersects, B within a constant number ($lstrp$) of bins from B', B directly below or to the left of B', or B equal to B' (see Figure 3). We note that identifying this region is essentially accomplished in **while** loop at line 18 and **for** loop at line 31, with the region understood to be the union of bins or Voronoi cells $B(m', n')$ of grid points in R at the end of **for** loop. Clearly, the region contains the graph of γ^*, and has the appearance of a strip whose shape evolves from one iteration to the next as it closely mimics the shape of the graph of γ^* (see Figure 3), thus it is referred to as an adapting strip. Finally, we note that at the end of **for** loop, γ^* in $\Gamma(R) \subseteq \Gamma(R')$ encoded in P for current iteration is obtained in line 38 with Procedure *DP* restricted to the region or adapting strip, a region that as just described depends on all previous γ^* functions from previous iterations. The last γ^* obtained is then, depending on $layrs$, optimal in $\Gamma(R)$, and, depending on $layrs$ and $lstrp$, in $\Gamma(R')$.

With γ^* as above during the execution of **while** loop at line 18 for iteration r, we note that since γ^* is in $\Gamma(R)$ then the number of bins $B(m', n')$ whose interiors the graph of γ^* intersects must be $O(NI + NJ)$, which is also the time required to find them one linear component of the graph at a time. Since $|R|$ at end of **for** loop at line 31 is then $O(lstrp) \cdot O(NI + NJ)$, i.e., $O(NI + NJ)$, complexity of Procedure *DP* at line 38 is then $O(NI + NJ)$, and since as mentioned above the sum of the NI's and NJ's is $O(N)$ and $O(M)$, respectively, then the complexity of *adapt-DP* must be $O(N + M)$, implying *adapt-DP* is linear.

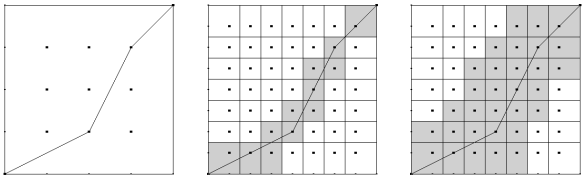


Figure 3. On left is γ^* from 2^{nd} iteration, $NI = NJ = 2^2 + 1 = 5$. In center, during 3^{rd} iteration, $NI = NJ = 2^3 + 1 = 9$; shaded bins are bins the interior of which γ^* intersects. On right, shaded bins form adapting strip in which next γ^* is computed. Each shaded bin is within 2 bins ($lstrp = 2$) from a bin whose interior current γ^* intersects, below or to the left of it or equal to it.

5. Applications and Experiments

In this section, we illustrate the effectiveness of Algorithm *adapt-DP* with several benchmarks and applications. We first compared it to *original-DP* [1, 9] and *fast-DP* [2] on synthetic applications. We examined both the computation times, and the accuracy of the solutions. Then we tested it on two important applications: elastic shape distances between 2d closed curves, and domain warping for alignment of functional data, specifically chromatograms. We report our findings in the respective subsections.

5.1. Synthetic Benchmarks

We evaluated *adapt-DP* using five synthetic curves in Figure 4 and γ functions shown in Figure 5. The γ functions were chosen to be difficult, having either small or steep gradients or both. We compared the results with those from *original-DP* and *fast-DP*. Given γ function, we reparametrized synthetic curve β_2 with it to obtain $\beta_1 = \beta_2(\gamma)$, and then with each algorithm tried to recover the discrete solution γ from the shape functions q_1, q_2 of β_1, β_2, respectively (see Subsection 5.2 for definition of shape functions), using $F(t, \gamma(t), \dot{\gamma}(t)) = \|q_1(t) - \sqrt{\dot{\gamma}(t)} q_2(\gamma(t))\|^2$ in (1). For various values of N (64, 128, 256, 512, 1024, 2048), and associated values of $layrs$ (64, 32, 16, 12, 12, 12, respectively), with $lstrp = 20$, we executed each algorithm, timed computations, and computed the L^2 error between the true solution γ^* and the computed γ, i.e., $\frac{1}{N-1}\left(\sum_{l=1}^{N-1}\left(\gamma(t_l) - \gamma^*(t_l)\right)^2\right)^{\frac{1}{2}}$. Algorithm *adapt-DP* not only computed reasonable γ^* functions for all synthetic curves (L^2 errors were less than 10^{-3}), but was much faster than the other algorithms for $N \geq 256$ (see Figure 5 and Table 1).

5.2. Computation of Elastic Shape Distances

An elastic shape framework was introduced in [9] for finding geodesics in the shape space of closed curves and computing geodesic distances between elements of that space. Let closed curves $\beta_i : [0, 1] \to \mathbb{R}^2, i = 1, 2$ be of class C^2 and unit length. As each β_i is closed, it sat-

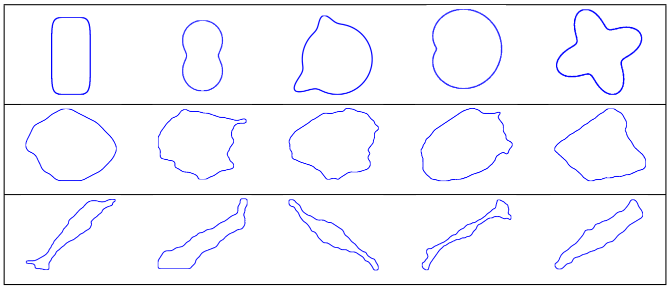


Figure 4. Curve examples used in the experiments. Synthetic curves: super ellipse, hippopede, bumps, limaçon, clover (top row); biological cell boundaries of type A and B (middle and bottom rows).

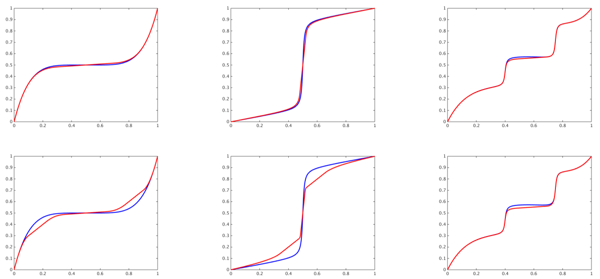


Figure 5. For γ^{flat} (left column in blue), *original-DP*, *fast-DP* with $d \approx 0.3\sqrt{2}$, and *adapt-DP* computed a reasonable γ^* (top left in red, L^2 error less than 10^{-3}), but *fast-DP* with $d \approx 0.2\sqrt{2}$ did not (bottom left, γ^* in red). The same can be said for γ^{steep} (middle column in blue). For γ^{bumpy} (right column in blue), *original-DP*, *fast-DP* with $d \approx 0.3\sqrt{2}$ and with $d \approx 0.2\sqrt{2}$ computed a reasonable γ^* (top right in red, L^2 error less than 10^{-3}). The same was true for *adapt-DP* which computed a slightly different γ^* (bottom right in red).

	$N =$	64	128	256	512	1024	2048
	layrs =	64	32	16	12	12	12
o-DP	*all* γ	0.49	1.26	1.00	2.07	8.48	34.3
f-DP	*all* γ	0.24	0.66	0.51	1.04	4.20	17.0
a-DP	γ^{flat}	0.65	0.67	0.27	0.29	0.57	1.20
	γ^{steep}	0.65	0.56	0.28	0.31	0.62	1.32
	γ^{bumpy}	0.81	1.04	0.37	0.36	0.70	1.46

Table 1. Times (in seconds) for limaçon with *original-DP* (*o-DP*), *fast-DP* (*f-DP*) with $d \approx 0.3\sqrt{2}$, and *adapt-DP* (*a-DP*). For *o-DP* and *f-DP*, the times depend only on N, not on γ, whereas for *a-DP*, the times depend on the shape of γ as well.

isfies $\beta_i(0) = \beta_i(1)$, $\dot{\beta}_i(0) = \dot{\beta}_i(1)$. We define $q_i(t) = \dot{\beta}_i(t)/\|\dot{\beta}_i(t)\|^{1/2}$ to be the shape function or square-root velocity function (SRVF) of β_i. Then the elastic shape distance between β_1 and β_2 is defined as the L^2 angle $\frac{\langle \hat{q}_1, \hat{q}_2 \rangle_{L^2}}{\|\hat{q}_1\|_{L^2} \|\hat{q}_2\|_{L^2}}$ between the optimally aligned SRVFs $\hat{q}_1$, $\hat{q}_2$, $\hat{q}_1(t) = R(\theta) q_1(t + t_0)$, $\hat{q}_2(t) = \sqrt{\dot{\gamma}(t)} q_2(\gamma(t))$, where t_0 is the optimal seed or starting point, $R(\theta)$ is the 2×2 rotation matrix defined by the optimal rotation angle θ, and γ is the optimal reparameterization function (see [3]). The triple (t_0, θ, γ) for optimal alignment is then obtained by minimizing the mismatch energy:

$$E(t_0, \theta, \gamma) = \int_0^1 \|R(\theta) q_1(t + t_0) - \sqrt{\dot{\gamma}(t)} q_2(\gamma(t))\|^2 dt. \tag{4}$$

Note that, for fixed t_0, θ, (4) is in the same form as (1) for $F(t, \gamma(t), \dot{\gamma}(t)) = \|R(\theta) q_1(t + t_0) - \sqrt{\dot{\gamma}(t)} q_2(\gamma(t))\|^2$. We use the trapezoidal rule to write a discretized version of the mismatch energy (4),

$$E^h(t_0, \theta, \vec{\gamma}) = h \sum_{l=1}^{N-1} \|R(\theta) q_1(t_l + t_0) - \sqrt{\dot{\gamma}_l} q_2(\gamma_l)\|^2, \tag{5}$$

essentially adapting (2) to this particular case.

In practice, the curves β_i are available as discrete sets of curve nodes. In order to obtain the continuous SRVFs q_i needed in (5), we first compute discrete derivatives $\dot{\beta}_i$ with centered finite differences, and then compute the corresponding q_i, which we interpolate with cubic splines.

The minimization of (5) to obtain the optimal triple $(t_0, \theta, \vec{\gamma})$ is the most critical part of the shape distance computation. Although a *globally* optimal triple is required to compute the correct theoretical distance, a practical optimization algorithm to accomplish this goal is not available. Instead, various local optimization approaches have been proposed. The approach in [9] is to loop through the starting point t_0 candidates, to compute for each t_0 candidate the optimal rotation angle θ (assuming identity for initial $\vec{\gamma}$), and then to compute the optimal reparameterization $\vec{\gamma}$ for each fixed pair (t_0, θ) with DP, which is the most expensive step as it is $O(N^2)$ for each pair. This optimization scheme is a direct search algorithm with total time complexity of $O(N^3)$. Faster iterative algorithms were proposed in [4] and [2, 3]. In [4], Huang et al. used Riemannian optimization to achieve faster computation times and improved minimization results as compared to the direct search approach in [9]. In [2, 3], Dogan et al. proposed an alternating optimization algorithm that optimizes (t_0, θ) with FFT, and $\vec{\gamma}$ with an iterative solver based on constrained nonlinear optimization using the interior point method and initialized with fast-DP. They were able to demonstrate subquadratic running times in experiments. In this paper, we would like to demonstrate the efficiency gains from our new DP algorithm when used to compute elastic shape distances. For this purpose, we adopted the $O(N^3)$ algorithm in [9], and replaced its $O(N^2)$ *original-DP* step with our $O(N)$ *adapt-DP*. We were able to show improvement by an order of magnitude in computation times, while still computing shape distances as good as the original algorithm.

In order to examine scalability with respect to N, we computed with algorithm in [9] the shape distance between two synthetic curves, hippopede and bumps (see Figure 4), using *original-DP* and *adapt-DP*. Results are given in Table 2. The shape distances from both approaches agree very well. But we see that computation times with *original-DP* grow cubically, whereas with *adapt-DP* grow quadratically. For $N = 256,\ 512$ we then computed 10×10 pairwise shape distance matrices for cell boundary curves in Figure 4 as well, and observed the same efficiency gains. Algorithm in [9] with *adapt-DP* had total computation time that is a fraction of what it had with *original-DP*: 17 min, 1 hr by *adapt-DP* vs 50 min, 7 hrs by *original-DP* for $N = 256, 512$ respectively. A 5×5 submatrix of the distance matrix for $N = 512$ is shown in Table 3.

Additionally, we verified that *adapt-DP* indeed handles nonuniform discretizations correctly and produces results as good as the uniform case. For this, we took two cell boundary curves in Figure 4, β_1, the rightmost curve in middle row, and β_2, the rightmost curve in bottom row. We resampled them uniformly with equal numbers of nodes $N_1 = N_2 = 257$, and with $F(t, \gamma(t), \dot{\gamma}(t)) = \|q_1(t) - \sqrt{\dot{\gamma}(t)}q_2(\gamma(t))\|^2$ in (1), computed $\vec{\gamma}$ with *adapt-DP* for optimal matching, and $E(\vec{\gamma})$, the value of mismatch energy for $\vec{\gamma}$. We repeated this experiment for the nonuniform discretization of these curves obtained with the two-step procedure in Section 2. Optimal energy values and computation times are given below. Numerical results of the nonuniform case are as good as those of the uniform case at half the cost of computation time.

	N_1	N_2	$E(\vec{\gamma})$	time
Uniform	257	257	0.3786	0.291s
Nonuniform	163	149	0.3628	0.138s

5.3. Function Alignment by Warping

In the context of elastic functional data analysis, a framework was introduced in [10] for domain warping of functions in order to align them optimally by matching critical features, such as peaks.

For $i = 1, 2$, let $f_i : [0, 1] \to \mathbb{R}$ be functions in an appropriate space of functions (e.g., the space of absolutely continuous functions), and let $q_i : [0, 1] \to \mathbb{R}$ be the square-root slope function (SRSF) of f_i: $q_i(t) = \text{sign}(\dot{f}_i(t))\sqrt{|\dot{f}_i(t)|}$, $t \in [0, 1]$ (see [10]). Note the SRSF is the form the SRVF takes as f_i is real-valued.

As established in [10] the warping function γ that makes $f_2(\gamma)$ the optimal alignment of f_2 to f_1 is obtained by minimizing the following energy with respect to γ:

$$E(\gamma) = \int_0^1 (q_1(t) - \sqrt{\dot{\gamma}(t)}q_2(\gamma(t)))^2 dt, \qquad (6)$$

	Timings for $Dist(hippopede, bumps)$			
	$N = 64$	128	256	512
original-DP	0.50	3.53	28.7	227
adapt-DP	0.57	2.35	9.7	40
	Timings for $Dist(bumps, hippopede)$			
original-DP	0.56	3.74	30.2	228
adapt-DP	1.04	2.88	10.3	46
	Values for $Dist(hippopede, bumps)$			
original-DP	1.052	1.043	1.042	1.037
adapt-DP	1.048	1.040	1.042	1.037
	Values for $Dist(bumps, hippopede)$			
original-DP	1.128	1.114	1.101	1.091
adapt-DP	1.129	1.114	1.101	1.091

Table 2. The numerical values and running times (in seconds) for the elastic shape distance between the two synthetic curves: hippopede and bumps for increasing N.

.580/.580	.545/.542	.557/.555	.510/.507	.543/.541
.509/.508	.526/.524	.498/.496	.478/.478	.541/.539
.540/.540	.620/.619	.580/.580	.515/.513	.585/.585
.596/.596	.541/.540	.580/.579	.565/.564	.582/.580
.497/.496	.545/.544	.512/.509	.468/.467	.542/.541

Table 3. Matrix of pairwise shape distances of type A (rows) and type B (columns) cells. The first and second values of a pair computed using *original-DP* and *adapt-DP*, respectively.

where as before γ is a diffeomorphism of $[0, 1]$ onto itself with $\gamma(0) = 0, \gamma(1) = 1, \dot{\gamma}(t) > 0$. Note that (6) is in the same form as (1) for $F(t, \gamma(t), \dot{\gamma}(t)) = (q_1(t) - \sqrt{\dot{\gamma}(t)}q_2(\gamma(t)))^2$.

In [12] the alignment of chromatograms using the framework in [10] described above was demonstrated on liquid chromatography-mass spectrometry data for a chromatographically complex metabolomic reference sample. Computational results were presented in [12] from aligning two chromatograms in this manner. The chromatograms were taken in immediate succession under the conventional high performance liquid chromatography (HPLC) protocol described in [12]. As reported there, for chromatograms having 1,000 points, the aligning took 10 seconds on a desktop computer. In this work, we addressed much larger chromatograms (19,000+ points) for which *original-DP* was impractical. We aligned such chromatograms in a few minutes using *adapt-DP* with $lstrp = 150$ and $layrs = 12$ (see Figure 6). Timings for these experiments are given below:

	Chromatogram 1	Chromatogram 2	time
Pair 1	19,713 pts	19,759 pts	180s
Pair 2	19,759 pts	26,474 pts	270s
Pair 3	19,693 pts	19,763 pts	172s

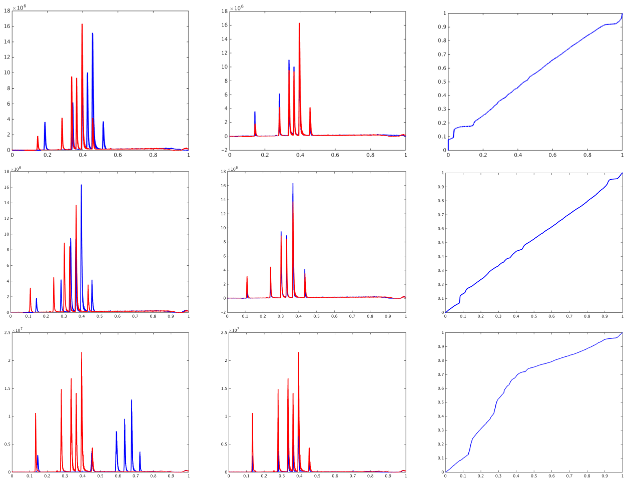


Figure 6. On left of each row, two chromatograms, one in blue and one in red of nonuniform time domains. In center, chromatograms in blue aligned to chromatograms in red after executions of *adapt-DP*. On right, plots of optimal piecewise warping functions.

6. Conclusions

In this paper, we propose a fast linear Dynamic Programming (DP) algorithm to compute optimal diffeomorphisms for elastic registration of curves. Although we cannot guarantee that it will always compute a globally optimal solution, we have observed very convincing results in our experiments. This algorithm which we call *adapt-DP* is based on ideas in [5, 8] in the context of graph bisection and dynamic time warping. We achieve considerable savings in computations and very favorable run times by restricting its search to thin strips around graphs of estimated solutions. It is essentially an iterative process that starts with a diffeomorphism computed at a very low resolution grid, projects at each iteration current diffeomorphism to one of double resolution using DP, and ends when a diffeomorphism of full resolution is obtained. This process runs with linear asymptotic time complexity with respect to the number of nodes on the given curves. We note, furthermore, *adapt-DP* has been implemented to allow for curves of possibly unequal and nonuniform discretized domains of definition. We use this flexibility to our advantage, to achieve further savings in computations, by not working with uniformly discretized curves, but with nonuniformly discretized curves of fewer nodes, as we concentrate nodes on parts with high curvature, and not so much on flat parts. We demonstrate the efficiency of *adapt-DP* with several examples. We achieve an order of magnitude gain in speed when we perform elastic shape analysis proposed in [9] with *adapt-DP*. We achieve even larger speed gains when we use *adapt-DP* for the alignment of chromatograms with large numbers of sample points. In particular, for chromatograms of 20,000 points, we show this can be done in approximately 3 minutes.

A copy of adapt-DP with example data files and usage instructions can be obtained from the link: `http://math.nist.gov/~JBernal/Fast_Dynamic_Programming.zip` We note that as currently implemented, *adapt-DP* uses only $F(t, \gamma(t), \dot{\gamma}(t)) = \|q_1(t) - \sqrt{\dot{\gamma}(t)} q_2(\gamma(t))\|^2$ in (1), $q_1, q_2 : [0, 1] \to \mathbb{R}^d$, $d = 1$ or 2.

References

[1] Code from Statistical Shape Analysis and Modeling Group, Florida State University. http://ssamg.stat.fsu.edu/downloads/ClosedCurves2D3D.zip. Accessed: 2014-06-20.

[2] G. Doğan, J. Bernal, and C. Hagwood. A fast algorithm for elastic shape distances between closed planar curves. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 4222–4230, June 2015.

[3] G. Doğan, J. Bernal, and C. Hagwood. FFT-based alignment of 2d closed curves with application to elastic shape analysis. In *Proceedings of the 1st International Workshop on Differential Geometry in Computer Vision for Analysis of Shape, Images and Trajectories (DIFF-CV) 2015, British Machine Vision Conference (BMVC)*, September 2015.

[4] W. Huang, K. A. Gallivan, A. Srivastava, and P.-A. Absil. Riemannian optimization for registration of curves in elastic shape analysis. *Journal of Mathematical Imaging and Vision*, 54(3):320–343, 2015.

[5] G. Karypis, R. Aggarwal, V. Kumar, and S. Shekhar. Multilevel hypergraph partitioning: Applications in VLSI domain. In *Proceedings of the Design and Automation Conference*, pages 526–530, 1997.

[6] W. Mio, A. Srivastava, and S. Joshi. On shape of plane elastic curves. *International Journal of Computer Vision*, 73(3):307–324, 2007.

[7] H. Sakoe and S. Chiba. Dynamic programming algorithm optimization for spoken word recognition. In *IEEE Trans. Acoustics, Speech, and Signal Proc.*, volume 26, 1978.

[8] S. Salvador and P. Chan. FastDTW: Toward accurate dynamic time warping in linear time and space. In *3rd Wkshp. on Mining Temporal and Sequential Data, ACM KDD '04*, August 2004.

[9] A. Srivastava, E. Klassen, S. Joshi, and I. Jermyn. Shape analysis of elastic curves in Euclidean spaces. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 33(7):1415–1428, 2011.

[10] A. Srivastava, W. Wu, S. Kurtek, E. Klassen, and J. Marron. Statistical analysis and modeling of elastic functions. *ArXiv:1103.3817*, 2011.

[11] G. Voronoi. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. *J. Reine Angew. Math.*, 133:97–178, 1908.

[12] W. E. Wallace, A. Srivastava, K. H. Telu, and Y. Simon-Manso. Pairwise alignment of chromatograms using an extended Fisher-Rao metric. *Analytica Chimica Acta 841*, pages 10–16, 2014.

Bernal, Javier; Dogan, Gunay; Hagwood, Robert.
"Fast Dynamic Programming for Elastic Registration of Curves."
Paper presented at the Proceedings of 2nd international workshop on differential geometry in
computer vision and machine learning (DIFF-CVML'16) in conjunction with CVPR 2016, Las Vegas, 2016., Las Vegas, NV, Jun 26-Jul 1, 2016.

Diversifying Network Services under Cost Constraints for Better Resilience against Unknown Attacks

Daniel Borbor[1], Lingyu Wang[1], Sushil Jajodia[2], and Anoop Singhal[3]

[1] Concordia Institute for Information Systems Engineering, Concordia University
{d_borbor,wang}@ciise.concordia.ca
[2] Center for Secure Information Systems, George Mason University
jajodia@gmu.edu
[3] Computer Security Division, National Institute of Standards and Technology
anoop.singhal@nist.gov

Abstract. Diversity as a security mechanism has received revived interest recently due to its potential for improving the resilience of software and networks against unknown attacks. Recent work shows diversity can be modeled and quantified as a security metric at the network level. However, such an effort does not directly provide a solution for improving the network diversity. Also, existing network hardening approaches are largely limited to handling previously known vulnerabilities by disabling existing services. In this paper, we take the first step towards an automated approach to diversifying network services under various cost constraints in order to improve the network's resilience against unknown attacks. Specifically, we provide a model of network services and formulate the diversification requirements as an optimization problem. We devise optimization and heuristic algorithms for efficiently diversifying relatively large networks under different cost constraints. We also evaluate our approach through simulations.

1 Introduction

Many critical infrastructures, governmental and military organizations, and enterprises have become increasingly dependent on networked computer systems today. Such mission critical computer networks must be protected against not only known attacks, but also potential zero day attacks exploiting unknown vulnerabilities. However, while traditional solutions, such as firewalls, vulnerability scanners, and IDSs, are relatively successful in dealing with known attacks, they are less effective against zero day attacks.

To this end, diversity has previously been considered for a security mechanism for hardening software systems against unknown vulnerabilities, and it has received a revived interest recently due to its potential for improving networks' resilience against known attacks. In particular, a recent work shows diversity can be modeled and quantified as a security metric at the network level [21]. However, the work does not directly provide a systematic solution for improving the network diversity under given cost constraints, which can be a challenging task for large and complex networks. On the other hand, existing efforts on network hardening (a detailed review of related work will be given later in Section 2) are largely limited to handling previously known vulnerabilities by disabling existing services.

Borbor, Daniel; Wang, Lingyu; Jajodia, Sushil; Singhal, Anoop.
"Diversifying Network Services under Cost Constraints for Better Resilience against Unknown Attacks."
Paper presented at the Lecture Notes in Computer Science, Trento, Italy, Jul 18-Jul 21, 2016.

In this paper, we propose an automated approach to diversifying network services under various cost constraints in order to improve the network's resilience against unknown attacks. Specifically, we devise a model of network services and their different instances by extending the resource graph model; such a model allows us to formulate the diversification requirements and cost constraints as an optimization problem; we apply optimization techniques to solve the formulated problems, and design heuristic algorithms to more efficiently handle larger networks. We evaluate our approach through simulations in order to study the effect of optimization parameters on accuracy and running time, and the effectiveness of optimization for different types of networks. In summary, the main contribution of this paper is twofold:

- To the best of our knowledge, this is the first effort on formulating the problem of network service diversification for improving the resilience of networks, which enables the application of existing optimization techniques and also provides a practical application for existing diversity metrics [21].
- As evidenced by the simulation results, the optimization and heuristic algorithms provide a relatively accurate and efficient solution for diversifying network services while considering various cost constraints. By focusing on zero day attacks, our work provides a complementary solution to existing network hardening approaches that focus on fixing known vulnerabilities.

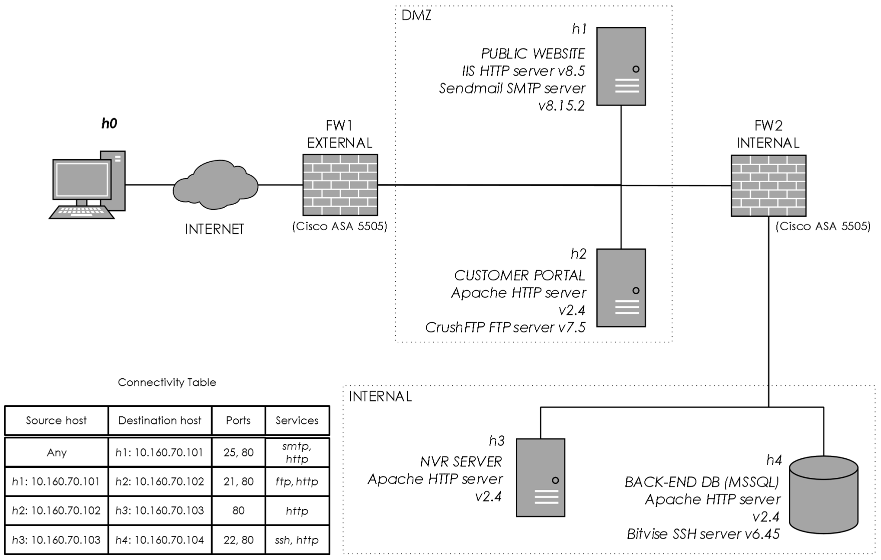
The remainder of this paper is organized as follows: The rest of this section first builds the motivation through a running example. Section 2 reviews related work. In Section 3, we present the model and formulate the optimization problem, and in Section 4 we discuss the methodology and show case studies. Section 5 shows simulation results and Section 6 concludes the paper.

1.1 Motivating Example

We present a motivating example to demonstrate that diversifying network services can be a tedious and error-prone task if done manually, even if the considered network is of a small size. Figure 1 shows a hypothetical network, which is roughly based on the virtual penetration lab described in [14]. Despite its relatively small scale, it mimics a typical enterprise network, e.g., with DMZ, Web server behind firewall accessible from public Internet, and a private management network protected by another firewall.

Specifically, the network consists of four hosts running one or more services allowing accesses from other hosts. We assume the two firewalls and other host-based mechanisms (e.g., personal firewalls or iptables) together enforce the connectivity described inside the connectivity table shown in the figure. We consider attackers on external hosts (represented as $h0$) attempting to compromise the database server ($h4$), and we assume the network is secured against known vulnerabilities (we exclude exploits and conditions that involve the firewalls).

To measure the network's resilience against unknown zero day attacks, we consider the *k-zero day safety metric* [17] (which will be referred to as $k0d$ from now on for simplicity), which basically counts how many distinct zero day vulnerabilities must exist and be exploited before an attacker may reach the goal. For simplicity, although the attacker may follow many paths to compromise $h4$, here we only consider the Web servers



Connectivity Table

Source host	Destination host	Ports	Services
Any	*h*1: 10.160.70.101	25, 80	*smtp, http*
*h*1: 10.160.70.101	*h*2: 10.160.70.102	21, 80	*ftp, http*
*h*2: 10.160.70.102	*h*3: 10.160.70.103	80	*http*
*h*3: 10.160.70.103	*h*4: 10.160.70.104	22, 80	*ssh, http*

Fig. 1. Example network.

as the initial targets. We can observe that there must exist at least two distinct zero-day vulnerabilities, one for the Apache server and one for the IIS server[1], and the attacker must exploit both in order to compromise $h4$. Finally, we assume the administrator has the option of replacing those Web servers with either an NGINX 1.9 or a Litespeed 5.0.14 Web server and each replacement will incur a given installation/maintenance cost (we will discuss the cost model in more details later in Section 3). Based on above assumptions, we may consider different use cases as follows.

- *Scenario 1:* The administrator aims to render the network as resilient as possible to zero-day attacks (which means to maximize the aforementioned $k0d$ metric).
- *Scenario 2:* He/she aims at the same goal as in above Scenario 1, but under the constraint that the overall diversification cost must be less than a given budget.
- *Scenario 3:* He/she aims at the same goal as in above Scenario 2, but under an additional constraint that at most two Web servers may be replaced.
- *Scenario 4:* He/she aims at the same goal as in above Scenario 3, but under an additional constraint that replacing the Web server should be given a higher priority.

Clearly, many more use cases may exist in practice than those listed above, and the solution may not always be straightforward even for such a small network. For example, while the administrator can easily increase the $k0d$ metric value to 4 under Scenario 1 (by having four different Web servers), the optimal solution in other scenarios will critically depend on the specific cost constraints and given budgets. Considering that the attacker may also follow other paths to attack (e.g., starting with SMTP, instead of Web, on h1), the problem becomes even more complicated. This shows the need for an automated approach, which will be the subject matter of the remainder of this paper.

[1] If different software are considered likely to share common vulnerabilities, a similarity-sensitive diversity metric may be needed [21].

2 Related Work

In general, the security of networks may be qualitatively modeled using attack trees [6, 7, 15] or attack graphs [2, 16]. A majority of existing quantitative models of network security focus on known attacks [20, 1], while few work have tackled zero day attacks [18, 17, 21] which are usually considered unmeasurable due to the uncertainties involved [12].

Early work on network hardening typically rely on qualitative models while improving the security of a network [16, 19]. Those work secure a network by breaking all the attack paths that an attacker can follow to compromise an asset, either in the middle of the paths or at the beginning (disabling initial conditions). Also. those work do not consider the implications when dealing with budget constraints nor include cost assignments, and tend to leave that as a separate task for the network administrators. While more recent works [1, 23] generally provide a cost model to deal with budget constraints, one of the first attempts to systematically address this issue is by Gupta et al. [10]. The authors employed genetic algorithms to solve the problem of choosing the best set of security hardening options while reducing costs. Dewri et a. [6] build on top of Gupta's work to address the network hardening problem using a more systematic approach. They start by analyzing the problem as a single objective optimization problem and then consider multiple objectives at the same time. Their work consider the damage of compromising any node in the cost model in order to determine the most cost-effective hardening solution. Later on, in [7] and in [22], the authors extrapolate the network hardening optimization problem as vulnerability analysis with cost/benefit assessment, and risk assessment respectively. In [13] Poolsappasit et al. extend Dewri's model to also take into account dynamic conditions (conditions that may change or emerge while the model is running) by using Bayesian attack graphs in order to consider the likelihood of an attack. Unlike our work, most existing work on network hardening are limited to known vulnerabilities and focus on disabling existing services.

There exist a rich literature on employing diversity for security purposes. The idea of using design diversity for tolerating faults has been investigated for a long time, such as the N-version programming approach [3], and similar ideas have been employed for preventing security attacks, such as the N-Variant system [5], and the behavioral distance approach [8]. In addition to design diversity and generated diversity, recent work employ opportunistic diversity which already exists among different software systems. For example, the practicality of employing OS diversity for intrusion tolerance is evaluated in [9]. More recently, the authors in [21] adapted biodiversity metrics to networks and lift the diversity metrics to the network level [21]. While those work on diversity provide motivation and useful models, they do not directly provide a systematic solution for improving diversity, which is the topic of this paper.

3 Model

We first introduce the extended resource graph model to capture network services and their relationships, then we present the diversity control and cost model, followed by problem formulation.

3.1 Extended Resource Graph

The first challenge is to model different resources, such as services (e.g., Web servers) that can be remotely accessed over the network, different instances of each resource (e.g., Apache and IIS), and the causal relationships existing among resources (e.g., a host is only reachable after an attacker gains a privilege to another host). For this purpose, we will extend the concept of *resource graph* introduced in [21], which is syntactically equivalent to attack graphs, but models network resources instead of known vulnerabilities as in the latter.

Specifically, we will define an *extended resource graph* by introducing the notion of *Service Instance* to indicate which instance (e.g., Apache) of a particular service (e.g., Web server) is being used on a host. Like the original resource graph, we only consider services that can be remotely accessed. The extended resource graph of the running example is shown in Figure 2 and detailed below.

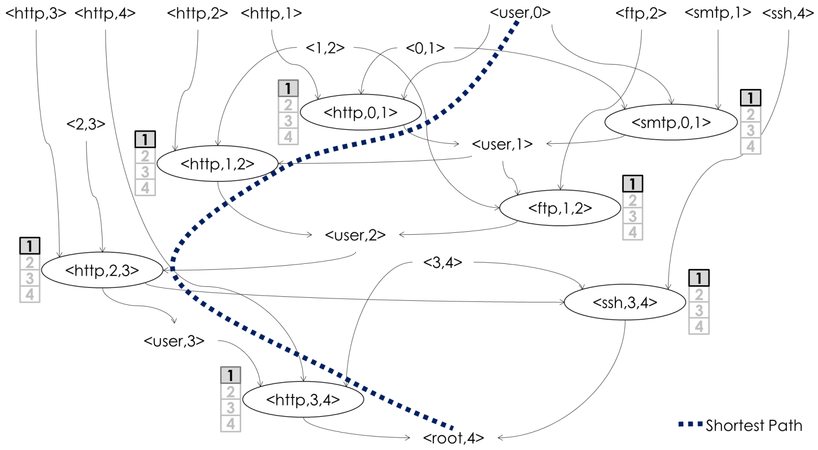


Fig. 2. The example network's resource graph

In Figure 2, each pair shown in plaintext is a security-related condition (e.g., connectivity $\langle source, destination\rangle$ or privilege $\langle privilege, host\rangle$). Each exploit node (oval) is a tuple that consists of a service running on a destination host, the source host, and the destination host (e.g., the tuple $\langle http, 1, 2\rangle$ indicates a potential zero day vulnerability in the $http$ service on host 2, which is exploitable from host 1). The small one-column table beside each exploit indicates the current service instance using a highlighted integer (e.g., 1 means Apache and 2 means IIS) and other potential instances in lighter text. The self-explanatory edges point from pre-conditions to an exploit (e.g., from $\langle 0, 1\rangle$ and $\langle http, 1\rangle$ to $\langle http, 0, 1\rangle$), and from the exploit to its post-conditions (e.g., from $\langle http, 0, 1\rangle$ to $\langle user, 1\rangle$).

A design choice here is whether to associate the service instance concept with a condition indicating the service (e.g., $\langle http, 2\rangle$ or the corresponding exploits (e.g., $\langle http, 1, 2\rangle$). While it is more straightforward to have the service instance defined as the property of a condition, which can then be inherited by the corresponding exploits, we have opted to define this property as a label for the exploit nodes in the graph, because this will make it easier to check the number of distinct services along a path, as we will see later. One complication then is that we must ensure all exploits with the same service and destination host (e.g., $\langle http, 1, 2\rangle$ and $\langle http, 3, 2\rangle$ to be associated with the same service instance.

Definitions 1 and 2 formally introduce these concepts.

Definition 1 (Service Pool and Service Instance). *Denote S the set of all services and Z the set of integers, for each service $s \in S$, the function $sp(.) : S \to \mathsf{Z}$ gives the service pool of s which represent all available instances of that service.*

Definition 2 (Extended Resource Graph). *Given a network composed of*

- *a set of hosts H,*
- *a set of services S, with the service mapping $serv(.) : H \to 2^S$,*
- *the collection of service pools $SP = \{sp(s) \mid s \in S\}$,*
- *and the labelling function $v(.) : E \to SP$, which satisfies $\forall h_s \in S \forall h'_s \in S, v(\langle s, h_s, h_d\rangle) = v(\langle s, h'_s, h_d\rangle)$ (meaning all exploits with common service and destination host must be associated with the same service instance, as explained earlier).*

let E be the set of zero day exploits $\{\langle s, h_s, h_d\rangle \mid h_s \in H, h_d \in H, s \in serv(h_d)\}$, and $R_r \subseteq C \times E$ and $R_i \subseteq E \times C$ be the collection of pre and post-conditions in C. We call the labeled directed graph, $\langle G(E \cup C, R_r \cup Ri), v\rangle$ the extended resource graph.

3.2 Diversity control and cost model

We employ the notion of *diversity control* as a model for diversifying one or more services in the resource graph. Since we represent the service instance using integers, it will be straightforward to regard each pair of service and destination host on which the service is running as an optimization variable, and formulate diversity control vectors using those variables as follows. We note that the number of optimization variables present in a network will depend on the number of conditions indicating services, instead of the number of exploits (since many exploits may share the same service instance, and hence the optimization variable). Since we only consider remotely accessible services in the extended resource graph model, we would expect in practice the number of optimization variables to grow linearly in the size of network (i.e., the number of hosts).

Definition 3 (Optimization Variable and Diversity Control). *Given an extended resource graph $\langle G, v\rangle$, $\forall e \in E,\ v(e)$ is an optimization variable. A diversity control vector is the integer valued vector $\boldsymbol{V} = (v(e_1), v(e_2), ..., v(e_{|E|})$.*

Changing the value of an optimization variable has an associated *diversification cost* and the collection of such costs is given in a *diversity cost matrix* in a self-explanatory manner. We assume the values of cost are assigned by security experts or network administrators. Like in most existing work (e.g., [6]), we believe an administrator can estimate the diversification costs based on monetary, temporal, and scalability criteria like *i*) installation cost, *ii*) operation cost, *iii*) training cost, *iv*) system downtime cost and, *v*) incompatibility cost. We define the diversity cost, diversity cost matrix, and the total diversity cost.

Definition 4 (Diversification Cost and Diversity Cost Matrix). *Given $s \in S$ and $sp(s)$, the cost to diversify a service by changing its service instance to another inside the service pool is called the diversification cost. The collection of all the costs associated with changing services in S are given as a diversity cost matrix DCM in which the element at i^{th} row and j^{th} column indicates the diversification cost of changing the i^{th} service instance to be the j^{th} service instance. Let $v_s(e_i)$ be the service associated with the optimization variable $v(e_i)$ and $\boldsymbol{V}_0$ the initial service instance values for each of the exploits in the network. The total diversification cost, C_d, given by the diversity vector $\boldsymbol{V}$ is obtained by*

$$C_d = \sum_{i=1}^{|E|} DCM_{v_s(e_i)}(\boldsymbol{V}_0(i), \boldsymbol{V}(i))$$

We note that the above definition of diversification cost between each pair of service instances has some advantages. For example, in practice we can easily imagine cases where the cost is not symmetric, i.e., changing one service instance to another (e.g. from Apache to IIS) carries a cost that is not necessarily the same as the cost of changing it back (from IIS to Apache). Our approach of using a matrix allows us to account for cases like this. Also, the concept can be used to specify many different types of cost constraints, which we will examine in the coming section. For example, an administrator who wants to restrict the total cost to diversify all servers running the $http$ service can do so by simply formulating the cost as the addition of all the optimization variables corresponding to $http$.

3.3 Problem formulation

As demonstrated in Section 1.1, the $k0d$ metric is defined as the minimum number of distinct resources on a single path in the resource graph [17]. For example, a closer look at Figure 2 shows that the $k0d$ value for our example network is 1. That is, an attacker needs only one zero-day vulnerability (in $http$ service instance 1) to compromise this network. The dashed line in Figure 2 depicts the shortest path that provides this metric value.

The $k0$ value can be increased by changing the service instances as long as we respect the available budget of cost. For example, consider a total budget of 78 units, and assume the costs to diversify the $http$ service from service instance 1 to 2, 3 or 4 be 78, 12, and 34 units, respectively. We can see that changing $\langle http, 2, 3\rangle$ from instance 1 to 2 would respect the budget, as well as increasing the $k0d$ value of the network to be 2. We may also see that this is not the optimal solution, since we could also replace $\langle http, 2, 3\rangle$ and $\langle http, 3, 4\rangle$ with instances 3 and 4, respectively, increasing $k0d$ to 3 and still respecting the budget. In the following, we formally formulate this as an optimization problem.

Problem 1 ($k0d$ Optimization Problem). Given an extended resource graph $\langle G, v\rangle$, find a diversity control vector $\boldsymbol{V}$ which maximizes $min(k0d(\langle G(\boldsymbol{V}), v\rangle))$ subject to the constraint $C \leq B$, where B is the availble budget and C is the total diversification cost as given in Definition 4.

Since our problem formulation is based on an extended version of the resource graph, which is syntactically equivalent to attack graphs, many existing tools developed for the latter (e.g., the tool in [11] has seen many real applications to enterprise networks) may be easily extended to generate the extended resource graphs we need as inputs. Additionally, our problem formulation assumes a very general budget B and cost C, which allows us to account for different types of budgets and cost constraints that an administrator might encounter in practice, as will be explained in the following section.

4 Methodology

This section details the optimization and heuristic algorithms used for solving the formulated diversification problem and describes a few case studies.

4.1 Genetic Algorithm Optimization

Inspired by [6], we also employ the genetic algorithm (GA) for our automated optimization approach. GAx1 provides a simple and robust search method that requires little information to search effectively in a large search space in contrast to other optimization methods (e.g., the mixed integer programming [4]). While the authors in [6] focus on disabling services, we focus on service diversification.

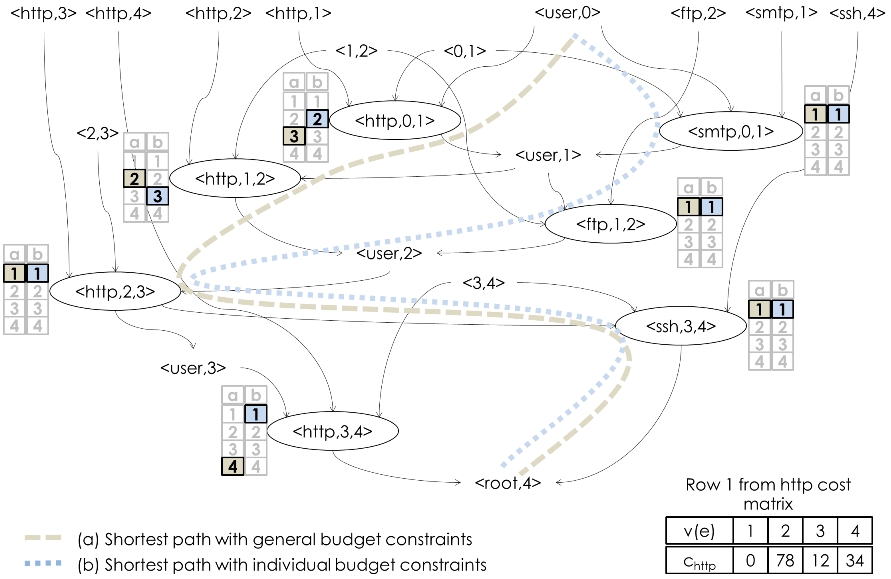
The extended resource graph is the input to our automated optimization algorithm where the function to be optimized (fitness function) is $k0d$ defined on the resource graph (later we will discuss cases where directly evaluating $k0$ is computationally infeasible). One important point to consider when optimizing the $k0$ function on the extended resource graph is that, for each generation of the GA, the graph's labels will dynamically change. This in turn will change the value of $k0d$, since the shortest path may have changed with each successive generation of the GA. Our optimization tool takes this into consideration. We also note one limitation here is that the optimization does not provide a priority if there are more than one shortest path that provide the optimized $k0d$ since the optimization only aims at maximizing the minimum $k0d$.

The constraints are defined as a set of inequalities in the form of $c \leq b$, where c represents one or more constraint conditions and b represents one or more budgets. These constraint conditions can be overall constraints (e.g. the total diversity cost C_d) or specific constraints to address certain requirements or priorities while diversifying services (e.g. the cost to diversify $http$ services should be less than 80% of the cost to diversify ssh). Those constraints are specified using the diversity control matrix.

The number of independent variables used by the GA (genes) are the optimization variables given by the extended resource graph. For our particular network hardening problem, the GA will be dealing with integer variables representing the selection of the service instances. Because $v(e)$ is defined as an integer, the optimization variables need to be given a minimum value and a maximum value. This range is determined by the number of instances provided in the service pool of each service. The initial service instance for each of the services is given by the extended resource graph while the final diversity control vector $\boldsymbol{V}$ is obtained after running the GA.

The population size that we defined for our tool was set to be at least the value of optimization variables (more details will be provided in the coming section). This way we ensure the individuals in each population span the search space. We ensure the population diversity by testing with different settings in genetic operations (like crossover and mutation). In the following, we discuss several test cases to demonstrate how the optimization works under different types of constraints. For all the test cases, we have used the following algorithm parameters: population size = 100, number of generations = 150, crossover probability = 0.8, and mutation probability = 0.2.

Test case A: $C_d \leq$ 124 units with individual constraints per service. We start with the simple case of one overall budget constraint ($C_d \leq$ 124). The solution provided by the GA is $\boldsymbol{V} = [3, 2, 1, 4, 1, 1, 1]$ (represented by label column a in Figure 3). The associated costs for $\boldsymbol{V}(1)$, $\boldsymbol{V}(2)$, and $\boldsymbol{V}(4)$ are 12, 78, and 34, respectively, and the test network's $k0d$ metric becomes 4 while keeping C_d within the budget ($C_d \leq$ 124).



v(e)	1	2	3	4
c_{http}	0	78	12	34

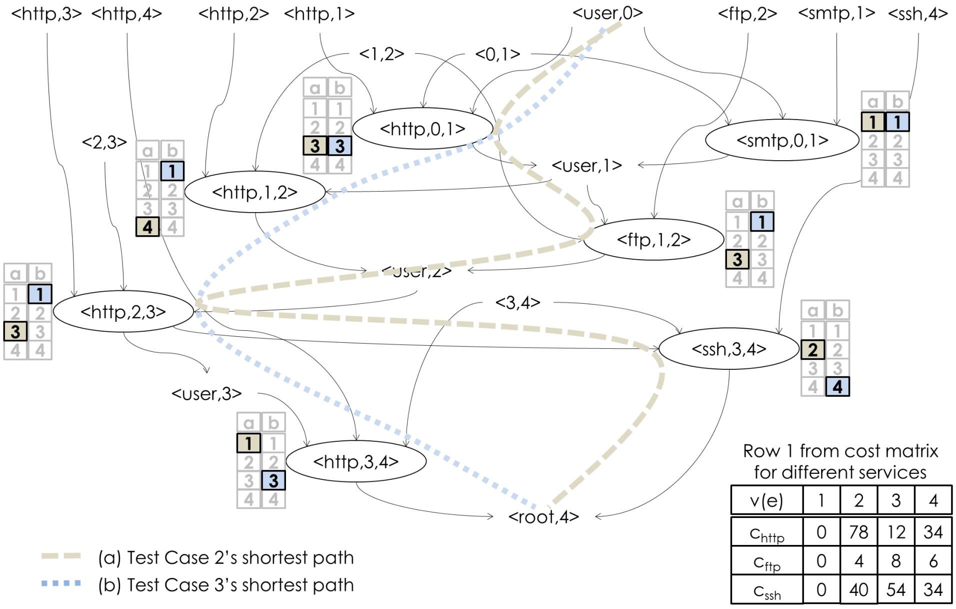
Fig. 3. Test case A: general and individual budget constraints.

On the other hand, if we assign individual budgets per services, while maintaining the overall budget $C_d \leq$ 124, the optimization results will be quite different. In this case, assume the budget to diversify the $http$ services cannot exceed 100 units ($c_{http} \leq$ 100); for ftp, it cannot exceed 3 units ($c_{ftp} \leq$ 3); for ssh, it cannot exceed 39 units ($c_{ssh} \leq$ 39); and finally, for $smtp$, it cannot exceed 50 units ($c_{smtp} \leq$ 50). The solution provided by the GA is a $\boldsymbol{V}$ vector where $\boldsymbol{V}(1) = 2$ and $\boldsymbol{V}(2) = 3$, with a cost of 78 and 12 units, respectively. The value of the $k0d$ metric rises to 3 with $C_d =$ 90. This total diversification cost satisfies both the overal budget constraint and each of the individual constraints per service.

From this test case, we can see that even with the minimum requeried budget to maximize the $k0d$ metric, additional budget constraints might not allow to achieve the maximum $k0d$ possible. We can see the result of running the GA for this test case in label column b in figure 3.

Test case B: $C_d \leq$ 124 units while $c_{http} + c_{ssh} \leq$ 100. While test case 1 shows how individual cost constraints can affect the $k0d$ metric optimization, in practice not all services may be of concern and some may have negligible cost. This test case models such a scenario by assigning a combined budget restriction for only the $http$ and ssh services, i.e., the cost incurred by diversifying these two services should not exceed 100 units.

The solution provided by the GA is $\boldsymbol{V} = [3, 4, 3, 1, 1, 3, 2]$ (lable column a in Figure 4). Since $\boldsymbol{V}(1)$ to $\boldsymbol{V}(3)$ deal with the $http$ service, we can see that the total incurred cost for $http$ is c_{http} =12+34+12=58 units. Because $\boldsymbol{V}(6)$ and $\boldsymbol{V}(7)$ are the only optimization variables that deal with the ftp and ssh services respectively, we can see that $c_{ftp} = 8$, and $c_{ssh} = 40$. The value of the $k0d$ metric rises from 1 to 3 by incurring a total cost of $C_d = 106$ units. The combined $http/ssh$ budget constraint of 100 units is also satisfied since $c_{http} + c_{ssh} = 98$ units.



Row 1 from cost matrix for different services

v(e)	1	2	3	4
c_{http}	0	78	12	34
c_{ftp}	0	4	8	6
c_{ssh}	0	40	54	34

Fig. 4. Test case B and test case C.

Test case C: $C_d \leq$ 124 units while $c_{http} \leq 0.8 \cdot c_{ssh}$. This final case deals with scenarios where some services might have a higher priority over others. The constraint in this test case is that the total incurred cost while diversifying the $http$ service should not exceed 80% of what is incurred by diversifying the ssh service.

The solution provided by the GA is $\boldsymbol{V}$ =[3,1,3,1,1,1,4] (see column b in figure 4). Here $\boldsymbol{V}(1)$ and $\boldsymbol{V}(3)$ have changed from service instance 1 to 3, while $\boldsymbol{V}(7)$ have changed from service instance 1 to 4. The incurred cost for the $http$ service is $c_{http} =$ 12+12=24 units and for the ssh service is $c_{ssh} =$ 34 units. While the value of the $k0d$ metric only rises from 1 to 2, the budget constraints are satisfied.

As seen from the above test cases, our model and problem formulation makes it relatively easy to apply any standard optimization techniques, such as the GA, to optimize the $k0d$ metric through diversity while dealing with different budget constraints.

4.2 Heuristic Algorithm

All the test cases described above rely on the assumption that all the attack paths are readily available. However, this is not always the case in practice. Due to the well known complexity that resource graphs have inherited from attack graphs due to their common syntax [21], it is usually computationally infeasible to enumerate all the available attack paths in a resource graph for large networks. Therefore, we design a heuristic algorithm to reduce the search complexity when calculating and optimizing the $k0d$ metric by only storing the m-shortest paths at each step, as depicted in Figure 5 and detailed below.

```
Procedure Heuristic_m-shortest
Input: Extended resource graph $\langle G, v \rangle$, goal condition $c_g$, number of paths $m$,
    diversified diversity control vector, $D$
Output: $\sigma(c_g)$
Method:
1.  Let $vlist$be any topological sort of G
5.  While all $vlist$ elements are unprocessed
6.        If $c \in C_I$ and $c$ is unprocessed
7.           Let $\sigma(c) = c$
8.           Mark $c$ as processed
9.        Else if $e \in E$ ($e$ is not processed) and $(\forall c \in C)((c, e) \in R_r \Rightarrow c$ is processed)
10.          Let $\{c \in C : (c, e) \in R_r\} = \{c_1, c_2, \ldots, c_n\}$
11.          Let $\alpha(e) = a_1 \cup a_2 \ldots \cup e : a_i \in \sigma(c_i),\ 1 \leq i \leq n$
13.          Let $\alpha'(ov(e)) = a'_1 \cup a'_2 \ldots \cup e : a'_i \vdash a_i,\ 1 \leq i \leq n$
12.          If $n > m$
13.             Let $\sigma(e) = ShortestM(\langle \alpha(e), \mid Unique(\alpha'[ov(e)]) \mid \rangle, m))$
14.          Else
15.             $\sigma(e) = a_1 \cup a_2 \ldots \cup e : a_i \in \sigma(c_i),\ 1 \leq i \leq m$
16.          Mark $e$ as processed
17.       Else ($c$ s.t. $(e, c) \in R_i$ and $c$ is unprocessed)
18.          If $(\forall e' \in E)((e', c) \in R_i \Rightarrow e'$ is processed)
19.             Let $\alpha(c) = \bigcup_{e' \text{ s.t. } (e', c) \in R_i} \sigma(e')$
20.             Let $\alpha'(c) = \bigcup_{e' \text{ s.t. } (e', c) \in R_i} \sigma(ov(e'))$
21.             If $length(\alpha(c)) > m$
22.                Let $\sigma(c) = ShortestM(\langle \alpha(c), \mid Unique(\alpha'[ov(c)]) \mid \rangle, m))$
23.             Else
24.                Let $\sigma(c) = \bigcup_{e' \text{ s.t. } (e', c) \in R_i} \sigma(e')$
25.          Mark $c$ as processed
26. Return $\sigma(c_g)$
```

Fig. 5. A Heuristic algorithm for calculating m-shortests paths

The algorithm starts by topologically sorting the graph (line 1) and then proceeds to go through each one of the nodes on the resource graph collection of attack paths, as set of exploits $\sigma()$, that reach that particular node. The main loop cycles through each unprocessed node. If a node is an initial conditions, the algorithm assumes that the node itself is the only path to it and it marks it as processed (lines 6-8). For each exploit e, all of its preconditions are placed in a set (line 10). The collection of attack paths $\alpha(e)$ is constructed from the attack paths of those preconditions (lines 10 and 11). In a similar way, $\sigma'(ov(e))$ is constructed with the function $ov()$ which, aside of using the exploits includes value of element of the diversity control vector that supervises that exploit.

If there are more than m paths to that node, the algorithm will use the function $Unique$ to first look for unique combinations of service and service instance in $\alpha'(ov(e))$. Then, the algorithm creates a dictionary structure where the key is a path from $\alpha(e)$ and the value is the number of unique service/service instance combinations given by each one of the respective paths in $\alpha'(ov(e))$. The function $ShortestM()$ selects the top m keys whose values are the smallest and returns the m paths with the minimum number of distinct combination of services and service instances (line 13). If there are less than m paths, it will return all of the paths (line 15). After this, it marks the node as processed (line 16). The process is similar when going through each one of the intermediate conditions (lines 17-24).

Finally, the algorithm returns the collection of m paths that can reach the goal condition c_g. It is worth noting that the algorithm does not make any distinction in whether or not a particular path has a higher priority over another when they share the same number of unique service/service instance combinations.

5 Simulations

In this section, we show simulation results. All simulations are performed using a computer equipped with a 3.0 GHz CPU and 8GB RAM in the Python 2.7.10 environment under Ubuntu 12.04 LTS and the MATLAB 2015a's GA toolbox. To generate a large number of resource graphs for simulations, we first construct a small number of seed graphs based on real networks and then generate larger graphs from those seed graphs by injecting new hosts and assigning resources in a random but realistic fashion (e.g., the number of pre-conditions of each exploit is varied within a small range since real world exploits usually have a constant number of pre-conditions). The resource graphs were used as the input for the optimization toolbox where the objective function is to maximize the minimum $k0d$ value subject to budget constraints. In all the simulations, we employ the heuristic algorithm described in section 4.2.

Figure 6 shows that the processing time increases almost linearly as we increase the number of optimization variables or the parameter m of the heuristic algorithm. The results show that the algorithm is relatively scalable with a linear processing time. On the other hand, the accuracy of the results is also an important issue to be considered. Here the accuracy refers to the approximation ratio between the result obtained using the heuristic algorithm and that of the brute force algorithm (i.e., simply enumerating and searching all the paths while assuming all services and service instances are different). For the simulations depicted in Figure 7, we settled for 50 iterations per graph per m-paths. The diversity control vector provided by the GA is used to calculate the accuracy. From the results, we can see that when m is greater or equal to 4 the approxi-

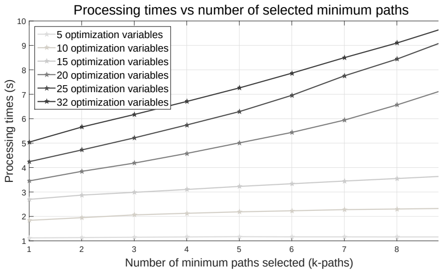


Fig. 6. Processing time.

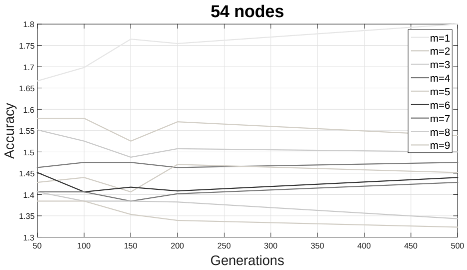


Fig. 7. Accuracy vs m (parameter of the heuristic algorithm).

mation ratio reaches an acceptable level. For the following simulations, we have settled with an m value of 6 and 100 generations.

Our simulations also showed that (detailed simulation results are omitted here due to page limitations), when no budget constraints are in effect, using the GA with a crossover probability of 80%, a mutation rate of 20%, and setting the number of generations to 50 will be sufficient to obtain good results. However, this is no longer the case when dealing with budget constraints. We have noticed that, by decreasing the crossover probability (and consequently increasing the mutation rate), we can reach a viable solution with less generations. We have therefore settled with a crossover probability of 40% which provides us with a fast (with less generations) way to converge to viable solutions. Additionally, our experiences also show that, when dealing with a diversity control vector (also known as a chromosome in the GA) of less than 100 variables (genes in the GA), the population size could be equal to the amount of variables in the diversity control vector; when dealing with a bigger number, the population size should be at least twice the amount of variables.

Figure 8 shows the results when the diversity control vector has different numbers of sevice instances to take from (i.e., different sizes of the service pools). In this simulation, we have picked graphs with a relative high difference in the length of the shortest path before and after all services are diversified using the algorithm (the maximum $k0d$ value is 16 and the minimum 3). We can see an increasing gain in the $k0d$ value after optimization, when more service instances are available. However, this trend begins to stall after a certain number (13). From this observation it can be inferred that the number of available service instances will affect the difference between the maximum $k0d$ value possible and the minimum $k0d$, but such an effect also depends on the size of the network (or the extended resource graph) and increasing the number of available service instances does not always help.

In Figure 9, we analyze the average gain in the optimized results for different sizes of graphs. In this figure, we can see that we have a good enough gain for graphs with a relatively high amount of nodes. As expected, as we increase the size of the graphs, the gain will decrease if we keep the same optimization parameters. For those simulations, we have used a population size of 300, 50 generations, and a crossover fraction of 50%. It is interesting to note that the decrease in gain is very close to being linear.

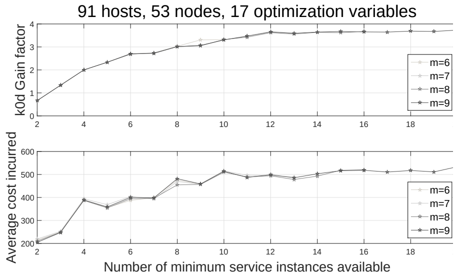


Fig. 8. The effect of the number of available service instances.

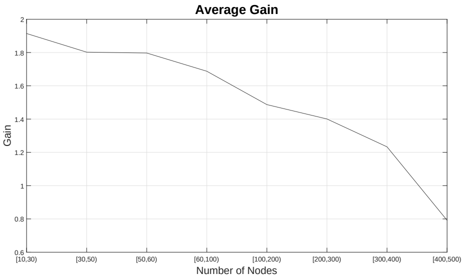


Fig. 9. The average gain vs the number of nodes.

Figure 10 and Figure 11 show the optimization results on different shapes of resource graphs. While it may be difficult to exactly define the depth of a resource graph, we have relied on the relative distance, i.e., the difference of the shortest path before and after all services are diversified. There is a relative linear increase in the gain as we increase the relative distance in the shortest path. While this does not provide an accurate description of the graph's shape, it does provide an idea of how much our algorithm can increase the minimum $k0d$ for graphs with different depths, as shown in Figure 10.

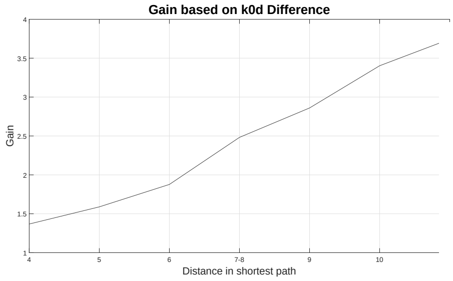


Fig. 10. Average gain based on relative distance of shortest path.

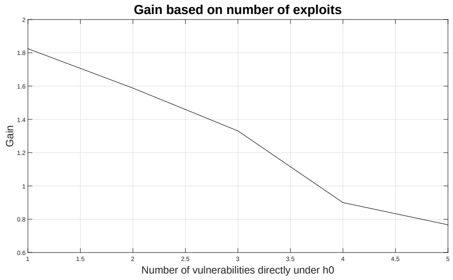


Fig. 11. Average gain based on directly reachable vulnerabilities.

Finally, in Figure 11, we can see the effect of the network's degree of exposure, which is defined as the number of exploits that are directly reachable by the attacker from the external host *h0*. As we increase the degree of exposure, the gain in optimization decreases in almost a linear way. That is, there will less room for diversification if the network is more exposed.

6 Conclusions

In this paper, we have formulated service diversity as an optimization problem and proposed an automated diversity-based network hardening approach against zero-day attacks. This automated approach used a heuristic algorithm that helped to manage the complexity of computing the $k0d$ value as well as limiting the time for optimization to an acceptable level. We have shown some sample cost constraints while our model and problem formulation would allow for other practical scenarios to be specified and optimized. We have tested the scalability and accuracy of the proposed algorithms through simulation results, and we have also discussed how the gain in the $k0d$ value will be affected by the number of available service instances in the service pools and different sizes and shapes of the resource graphs.

We discuss several aspects of the proposed automated optimization technique where additional improvements and evaluations can be done.

- While this paper focuses on diversifying services, a natural future step is to integrate this approach with other network hardening options, such as addition or removal of services, or relocating hosts or services (e.g., firewalls).
- This study has relied on a simplified model by assuming all service instances to be completely different from each another and all service instances are equally likely to be exploited. A possible future research direction would be to model the degree of difference (or similarity) between the different types of service instances.
- We have assumed an abstract cost model in this paper and an important direction is to elaborate the model from different aspects of potential cost for diversifying network resources.
- We will also consider other optimization algorithms in addition to GA in searching for more efficient and effective solutions to our problem.

Disclaimer Commercial products are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the identified products are necessarily the best available for the purpose.

References

1. Massimiliano Albanese, Sushil Jajodia, and Steven Noel. Time-efficient and cost-effective network hardening using attack graphs. In *Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on*, pages 1–12. IEEE, 2012.
2. Paul Ammann, Duminda Wijesekera, and Saket Kaushik. Scalable, graph-based network vulnerability analysis. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 217–224. ACM, 2002.
3. A. Avizienis and L. Chen. On the implementation of n-version programming for software fault tolerance during execution. In *Proc. IEEE COMPSAC*, volume 77, pages 149–155, 1977.
4. H Md Azamathulla, Fu-Chun Wu, Aminuddin Ab Ghani, Sandeep M Narulkar, Nor Azazi Zakaria, and Chun Kiat Chang. Comparison between genetic algorithm and linear programming approach for real time operation. *Journal of Hydro-environment Research*, 2(3):172–181, 2008.
5. B. Cox, D. Evans, A. Filipi, J. Rowanhill, W. Hu, J. Davidson, J. Knight, A. Nguyen-Tuong, and J. Hiser. *N-variant systems: A secretless framework for security through diversity*. Defense Technical Information Center, 2006.

6. Rinku Dewri, Nayot Poolsappasit, Indrajit Ray, and Darrell Whitley. Optimal security hardening using multi-objective optimization on attack tree models of networks. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 204–213. ACM, 2007.
7. Rinku Dewri, Indrajit Ray, Nayot Poolsappasit, and Darrell Whitley. Optimal security hardening on attack tree models of networks: a cost-benefit analysis. *International Journal of Information Security*, 11(3):167–188, 2012.
8. D. Gao, M. Reiter, and D. Song. Behavioral distance measurement using hidden markov models. In *Recent Advances in Intrusion Detection*, pages 19–40. Springer, 2006.
9. M. Garcia, A. Bessani, I. Gashi, N. Neves, and R. Obelheiro. OS diversity for intrusion tolerance: Myth or reality? In *2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN)*, pages 383–394, 2011.
10. Mukul Gupta, Jackie Rees, Alok Chaturvedi, and Jie Chi. Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach. *Decision Support Systems*, 41(3):592–603, 2006.
11. S. Jajodia, S. Noel, and B. O'Berry. Topological analysis of network attack vulnerability. In V. Kumar, J. Srivastava, and A. Lazarevic, editors, *Managing Cyber Threats: Issues, Approaches and Challenges*. Kluwer Academic Publisher, 2003.
12. John McHugh. Quality of protection: measuring the unmeasurable? In *Proceedings of the 2nd ACM workshop on Quality of protection*, pages 1–2. ACM, 2006.
13. Nayot Poolsappasit, Rinku Dewri, and Indrajit Ray. Dynamic security risk management using bayesian attack graphs. *Dependable and Secure Computing, IEEE Transactions on*, 9(1):61–74, 2012.
14. Penetration testing virtual labs. https://www.offensive-security.com/offensive-security-solutions/virtual-penetration-testing-labs/, Sep, 2015.
15. Indrajit Ray and Nayot Poolsapassit. Using attack trees to identify malicious attacks from authorized insiders. In *ESORICS 2005*, pages 231–246. Springer, 2005.
16. Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, and Jeannette M Wing. Automated generation and analysis of attack graphs. In *Security and privacy, 2002. Proceedings. 2002 IEEE Symposium on*, pages 273–284. IEEE, 2002.
17. Lingyu Wang, Sushil Jajodia, Anoop Singhal, Pengsu Cheng, and Steven Noel. k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities. *Dependable and Secure Computing, IEEE Transactions on*, 11(1):30–44, 2014.
18. Lingyu Wang, Sushil Jajodia, Anoop Singhal, and Steven Noel. k-zero day safety: Measuring the security risk of networks against unknown attacks. In *ESORICS 2010*, pages 573–587. Springer, 2010.
19. Lingyu Wang, Steven Noel, and Sushil Jajodia. Minimum-cost network hardening using attack graphs. *Computer Communications*, 29(18):3812–3824, 2006.
20. Lingyu Wang, Anoop Singhal, and Sushil Jajodia. Measuring the overall security of network configurations using attack graphs. In *Data and Applications Security XXI*, pages 98–112. Springer, 2007.
21. Lingyu Wang, Mengyuan Zhang, Sushil Jajodia, Anoop Singhal, and Massimiliano Albanese. Modeling network diversity for evaluating the robustness of networks against zero-day attacks. In *ESORICS 2014*, pages 494–511. Springer, 2014.
22. Shuzhen Wang, Zonghua Zhang, and Youki Kadobayashi. Exploring attack graph for cost-benefit security hardening: A probabilistic approach. *Computers & security*, 32:158–169, 2013.
23. Beytullah Yigit, Gurkan Gur, and Fatih Alagoz. Cost-aware network hardening with limited budget using compact attack graphs. In *Military Communications Conference (MILCOM), 2014 IEEE*, pages 152–157. IEEE, 2014.

COMPARISON OF REGISTRATION METHODS FOR MOBILE MANIPULATORS

ROGER BOSTELMAN[1,2], ROGER EASTMAN[3], TSAI HONG[1],
OMAR ABOUL ENEIN[1], STEVEN LEGOWIK[4], SEBTI FOUFOU[5]
[1]*National Institute of Standards and Technology, Engineering Laboratory, Intelligent Systems Division, Gaithersburg, MD, USA*
[2]*Le2i Lab, Université de Bourgogne, BP 47870, 21078 Dijon, France*
[3]*Loyola University Maryland, Baltimore, MD, USA*
[4]*Robotic Research*, LLC, Gaithersburg, MD, USA
[5]*CSE Dept, College of Engineering, Qatar University, Qatar*.

Mobile manipulators can be effective, efficient, and flexible for automation on the factory floor but will need safety and performance standards for wide adoption. This paper looks at a specific area of performance standards [1] for docking and workpiece registration, with the intent of evaluating how quickly, repeatably, and accurately a mobile manipulator end effector can be aligned with a known physical target to facilitate peg-in-hole insertion tasks. To evaluate mobile manipulator docking, we conducted experiments with an automated guided vehicle (AGV)-mounted arm in a laboratory space equipped with an extensive optical tracking system and a standardized test piece (artifact) simulating an industrial assembly. We experimented with different strategies and sensors for registration and report on these approaches.

1. Introduction

Mobile manipulators (i.e., robot arms onboard mobile robotic bases) hold promise in industrial applications* for flexible and reconfigurable automation and are now being marketed at industrial material handling exhibitions as useful tools [2, 3]. Typical applications currently being considered for mobile manipulators are: i) unloading trucks [4], ii) bagged-goods (e.g., dog food bags) handling, iii) conveyer loading/unloading, iv) picking canned and boxed goods from shelves in supermarkets, and v) delivering, placing, and manipulating semiconductor wafer pods within wafer fabrication facilities [5]. The first four applications have looser constraints on the mobile manipulator pose (position and orientation) and do not require precise alignment with the workspace. Vision is integrated into these

* Disclaimer: NIST does not endorse products discussed within this paper nor manufacturers of these products. Products mentioned are for information purposes only and are not expressed as an endorsement for them or their manufacturer.

Bostelman, Roger; Eastman, Roger; Hong, Tsai; Enein, Omar; Legowik, Steven; Foufou, Sebti.
"Comparison of Registration Methods for Mobile Manipulators."
Paper presented at the Climbing and Walking Robots (CLAWAR) 2016 Workshop on
Collaborative Robots for Industrial Applications, London, United Kingdom, Sep 12-Sep 16, 2016.

systems to position a vacuum gripper to pick up the box, bag, or metal can in the manipulator's workspace. However, the last application, wafer pod manipulation, and other assembly-type operations, (e.g., peg-in-hole), require much tighter tolerances on positioning from the mobile manipulator.

The National Institute of Standards and Technology (NIST) Robotic Systems for Smart Manufacturing Program [6] is currently researching, among other topics, both automatic guided vehicle (AGV)/mobile manipulator performance and vision performance standards [7]. The program develops and deploys advances in measurement science by improving performances of robotic systems to achieve dynamic production for assembly-centric manufacturing.

Assembly operations performed by a mobile manipulator require accurate registration to the workpiece. Registration refers to the process of measuring and mapping the feedback from one system (e.g., mobile manipulator) to the model of another (e.g., artifact), correcting for differences in resolution, scale, direction, and timing. [8] 'Calibration' is instrument (e.g., camera) adjustment or output correlation of the instrument readings with its known accuracy. These two terms are sometimes interchanged in the literature. Various registration methods have been researched, including:

- Quick Reference (QR) codes [9] combined with calibrated vision [10] - tracking error: under 20 mm, maximum errors: 45 mm at the largest camera-target distance.
- QR codes for mobile robot registration and end effector error [11] - maximum positional repeatability: 1.1 mm (one point) to 4.0 mm (multiple points).
- High-precision calibration - average errors based on the Tsai hand-eye calibration combined with a high-speed calibration - average errors: ± 0.1 mm and ± 0.1° - based on a combination of laser triangulation and image processing [12].
- Constrained manipulator endpoint to a single contact point while executing manipulator motion where manipulator joint angles are read to develop a calibration model [13].
- Touch probing using peg-in-hole and particle filter solutions [14, 15].

This paper describes three alternative methods for registering mobile manipulators to a workpiece. The first builds upon [11] from Aalborg University where QR codes were used in combination with vision processing. The second and third use 'fine' and 'bisect' search methods using a laser retroreflector to determine fiducial location with respect to the mobile manipulator. Experiments and experimental results are then described for each of these calibration alternatives.

2. Registration Methods

Registration of a mobile manipulator with a workpiece can be performed using a number of techniques, as briefly described in the introduction. If the accuracy requirements of the task are low, then simple navigation of the base to the desired pose may be adequate. However, we assume the manipulator accuracy requirements are greater than the base's accuracy and more information is required for a suitable transformation between the manipulator and workpiece coordinate systems. The following subsections describe three non-contact methods tested at NIST for registering a mobile manipulator to a workpiece - detection of QR codes using vision and two search methods using a laser retroreflector and reflective fiducials. Future research may combine the registration methods by using a laser spot detection method as described in [17 and 18].

2.1. *Visual Fiducials*

Visual fiducial systems allow for six degrees-of-freedom (6DOF) positional tracking of fiducial targets, or tags. Since these systems are well-developed, and can be implemented with open source software, inexpensive cameras, and virtually free printed targets, they have a number of advantages for use in robotics research and testing procedures for industrial robot evaluation and validation.

In this study, we reviewed fiducial systems commonly labeled as AR, or augmented reality. These systems include: ARTag, April tags, ARToolKit, and ALVAR [19]. We conducted experiments using the "A software Library for creating Virtual and Augmented Reality" or ALVAR version because of its integration with Robot Operating System (ROS). Integration with ROS allowed the use of ROS preprocessing, visualization, and message-passing facilities. Like the other systems, ALVAR uses rectangular black and white targets with a black outer square for location, and an internal matrix of squares that codes the identity of the target. Other fiducial targets used include standard camera calibration targets (i.e., checkerboards), QR codes, and application-specific targets.

ALVAR and similar systems have advantages in flexibility and cost over other 6DOF tracking systems that may require more expensive and extensive installations. We need to understand robustness, working range and orientations, accuracy, and response time for ALVAR use in testing procedures and standards. These needs do not have universal solutions since the system performance depends on implementation details. Robustness depends on occlusion and camera details; working range depends on target size, camera resolution, and camera focal length; response time depends on camera frame rate, resolution, and computer processing unit speed; and ultimate accuracy depends on all these factors, including target motion speed relative to frame rate.

2.2. *Fine and Bisect Search Methods*

A ‘fine search’ method was described in [18 and 20] as it evolved; it is included in this paper to focus on the registration aspect. The method uses a laser retroreflector detector carried by the manipulator to detect reflective fiducials attached to the reconfigurable mobile manipulator apparatus (RMMA). The RMMA is a metal plate with fiducial mount points at precise locations. The fiducial is a collimated reflector on a base that attaches to the RMMA.

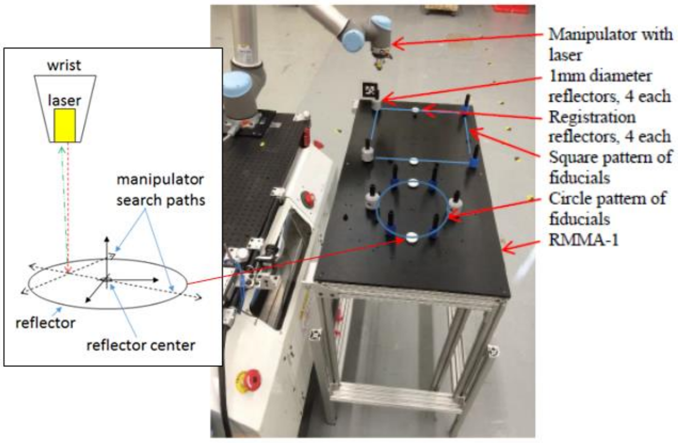
A computer aided design model of paths and docking points was used by a vehicle control program to move the AGV from one docking pose to another near the RMMA. The vehicle control program positioned the vehicle at various orientations with respect to the RMMA and the manipulator program corrected for vehicle pose allowing it to register with pre-taught targets using fine and ‘bisect’ search methods described here.

Two pairs of fiducials were positioned at 1) two corners of a 457 mm square pattern of four fiducials and 2) at opposing points along a 305 mm diameter circle pattern of eight fiducials. The fine search originally used a circular search [18] and was tested only on the square pattern. However, it was quickly discovered that fiducial edges were detected causing a potential for the registration to be skewed and increased search steps caused the laser to pass over the fiducial without detecting it.

In [20], a square fine search method was tested. The ‘square search’ is a sequence of points in a spiral pattern on a square grid. Each step was 0.5 mm, where the smaller step size and the use of 1 mm and 2 mm fiducials minimized previous issues. Figure 1 (a) shows a graphic of the square search method and Figure 1 (b) shows the RMMA (black table). The gray housings each include a camera iris that is used to change the fiducial detection diameter. This method works relatively well for aligning the mobile manipulator with the workpiece. However, errors in the mobile base pose measurement can cause a lengthy initial registration search.

For the bisect method, the detection of two, relatively large (42 mm diameter) reflectors was performed before the fine search method. All reflectors were the same type micro-reflector. After detecting the large reflector, a bisecting search pattern determined the center of the reflector with 0.5 mm steps along relative X- and Y- axes to the manipulator base.

The reflector diameters were large enough that no initial search was required to locate them, despite the measured maximum 13.3 mm error in the mobile base pose. Figure 1 (a) shows a concept drawing of the bisect method and Figure 1 (b) shows the mobile manipulator positioned next to the RMMA, the RMMA square and circle patterns, and the large reflectors within each pattern. Once the center of the large reflector was located, the manipulator began a fine search of the 2 mm fiducials using the square search method.


wrist
laser
manipulator search paths
reflector
reflector center
Manipulator with laser
1mm diameter reflectors, 4 each
Registration reflectors, 4 each
Square pattern of fiducials
Circle pattern of fiducials
RMMA-1

a b

Figure 1 (a) Bisection search concept, (b) the mobile manipulator positioned next to the RMMA, the RMMA square and circle patterns, and the large reflectors within each pattern.

3. Experiments and Results

3.1. *Visual Fiducials*

To evaluate and validate the use of visual fiducial targets, we conducted two sets of experiments using the ALVAR implementation and a 17 mm machine vision camera with a resolution of 1296 pixels x 964 pixels and a fixed 4.5 mm focal length lens.

The first set of experiments looked at the static repeatability of the ALVAR system when the target was moved to static positions by a pan-tilt mechanism. A 200 mm x 200 mm target was mounted on a pan-tilt unit. For the experiments, the pan-tilt was moved systematically throughout its range and allowed to settle before static measurements. The camera viewed the target from a separation distance of 800 mm to 1000 mm as the target was systematically moved to 26 positions of differing tilt and pan. For each position, 306 measurements were taken over 30 s. We calculated the root-mean-square deviation (RMSD) of the measurements to see if ALVAR gave consistent results. Repeatable measurements indicate systemic biases can be corrected by calibration.

We found that the maximum difference from the mean in any one position in any dimension was 0.8 mm (along the Z-axis), and the maximum angular error (in angle axis representation) was 0.18°. Each individual measurement was single shot with no averaging or filtering across measurements. From initial results of sub-millimeter repeatability in position, and fractional angular repeatability, we judge that the basic capabilities of ALVAR are adequate as a subsystem in workpiece registration.

In the second set of visual fiducial experiments, we integrated ALVAR with the systems on an AGV docking with the RMMA. Spacing between the RMMA square and circle patterns was 508 mm. The camera, which was onboard the AGV, repeatedly measured the AGV positioning at the square and circle patterns, and communicated the position to the robot controller.

3.2. *Fine and Bisect Search methods*

The RMMA was set up as shown in Figure 1 (b) for the circle pattern with 1 mm diameter registration fiducials. The circle used 1 mm diameter fiducials and the square used 3 mm diameter fiducials. The 3mm fiducials were hypothesized to achieve faster registration although this was not the case. The AGV control program moved the AGV from a home position away from the RMMA to the first pose pre-determined by the AGV control program. Upon completion of the pattern detection for the first pose, the AGV moved to the second pose, and so forth. Only the first six vehicle poses were completed for the 'fine search' method due to the long registration time. The 3 mm fiducial had the highest average number of search steps at 869 with 1921 maximum steps and 1740 s causing an average search time of 360 s with a maximum of 893 s. The root-mean-square deviation (RMSD) from the mean was 776 steps (403 s).

The 'bisect search' method experiment consisted of locating the mobile manipulator in the same manner as in the fine search method. The RMMA was set up as shown in Figure 1 (b) with the circle and square patterns both using 42 mm diameter registration fiducials. After setup, the experiment was run for all 10 different mobile manipulator poses and repeated five times for a total of 50 poses. The results shown in Table 1 include only the detection of the first 2 mm reflector for each pattern after bisect registration. The bottom of Table 1 shows a summary of all tests averaged over the 50 measurements and includes the average number of steps for the 2 mm reflectors and shows the RMSD from the mean.

Table 1: Mobile manipulator registering to the RMMA using the bisect search method.

AGV Position Number	Pose Angle	Pattern	Average num. of search steps to register	Total bisect + fine search time to register (s)
1	90°	circle	0	86
2	315°	square	6	89
3	0°	circle	0	86
4	0°	square	0	86
5	45°	circle	0	86
6	90°	square	0	86
7	135°	circle	0	86
8	225°	square	0	86
9	270°	circle	0	86
10	270°	square	12	92

Mean Search Steps/Time (s)	1.8 / 0.8	RMSD Search Steps/Time (s)	3.8 / 1.8

4. Conclusions

Experimental results reported for visual fiducials are consistent with the various registration methods from the literature. Under optimal conditions, we estimated repeatability of a visual fiducial at under 1 mm and 0.2° from a single image. From initial results we expect that basic capabilities of ALVAR are adequate as a subsystem in workpiece registration. The second ALVAR experiment provided successful integration with the mobile manipulator. Given other elements in the system, including calibration of camera-to-base, and base-to-arm, and the propagation of error, we would expect total error for the system to be higher.

The fine search method experiments resulted in a high number of search steps and time (average steps: 776, average/maximum time: 360 s/893 s) to register the mobile manipulator. When using the bisect method prior to the fine search, the total bisect plus fine search steps/time was a maximum of 184 steps/86 s or nearly 90% less time than using only the fine search method. Larger bisect search steps, among many other improvements, could be used although would increase the number of registration search steps on the 1 mm or 2 mm fiducials to a potentially unknown amount. Future registration tests will combine the visual fiducial with the search methods to minimize the search time.

References

1. ASTM Committee F45, WK48955 working document, Navigation: Defined Space, April 2016.
2. ProMat 2015, Material Handling Ind. of America, Chicago, IL, March 2015.
3. Modex 2016, Material Handling Ind. of America, Atlanta, GA, April 2016
4. "Yaskawa Motoman MH80 robot unloading trucks - Wynright Corp.," http://www.youtube.com/watch?v=8wngL0BnF_4, June 2013.
5. Adept Lynx Handler-Semi, http://www.adept.com/products/mobile-robots/mobile-transporters/handler-semi/general
6. National Institute of Standards and Technology, Robotic Systems for Smart Manufacturing Program, http://www.nist.gov/el/isd/ms/rssm.cfm, April 2016.
7. ASTM E2919-14, http://www.astm.org/Standards/E2919.htm, April 2016.
8. Tools for Robotics in SME Workcells: Challenges and Approaches for Calibration and Registration, NISTIR 8093, National Institute of Standards and Technology, Gaithersburg, MD, 2015.
9. R. Andersen, O. Madsen, T. Moeslund, "Hand-Eye of Depth Cameras based on Planar Surfaces", Abstract from Int'l Workshop on Intell. Robot Assistants, Padova, Italy, 2014.
10. B. Hamner, S. Koterba, J. Shi, R. Simmons, S. Singh, "An autonomous mobile manipulator for assembly tasks" *Auton. Robot* **28**: 131–149 (2010).
11. R. Andersen, J. Damgaard, O. Madsen, T. Moeslund, "Fast calibration of industrial mobile robots to workstations using QR codes." 44th Int'l Symp. Robotics (ISR), pp. 1-6. IEEE, 2013.
12. M. Hvilshøj, et al., "Calibration techniques for industrial mobile manipulators: Theoretical configurations and best practices." Robotics (ISR), 2010 41st International Symposium on and 2010 6th German Conference on Robotics (ROBOTIK). VDE, 2010.
13. M. Meggiolaro, G. Scriffignano, S. Dubowsky, "Manipulator Calibration Using A Single Endpoint Contact Constraint", Proceedings of DETC2000: 2000 ASME Design Engineering Technical Conference, DETC2000/MECH-14129, Baltimore, MD, September 2000.
14. S. Chhatpar, M. Branicky, "Localization for Robotic Assemblies Using Probing and Particle Filtering", Proc. of the 2005 IEEE/ASME Int'l Conf. on Advanced Intelligent Mechatronics, Monterey, CA, USA, 24-28 July 2005.
15. Y. Taguchi, T. Marks, J. Hershey, "Entropy-Based Motion Selection for Touch-Based Registration Using Rao-Blackwellized Particle Filtering", TR2011-067, September 2011.
16. M. Mesko, S. Toth, "Laser Spot Detection", Journal of Information, Control and Management Systems, **11**, No. 1 (2013).
17. A. Krstinic, K. Skein, I. Milatic, "Laser Spot Tracking Based On Modified Circular Hough Transform and Motion Pattern Analysis", *Sensors*, **14**, 20112-20133; ISSN 1424-8220, (2014).
18. R. Bostelman, T. Hong, J. Marvel, "Performance Measurement of Mobile Manipulators", SPIE 2015, Baltimore, MD, April 2015.
19. N. Macias, J. Wen, "Vision guided robotic block stacking", IEEE/RSJ Int'l Conf. Intelligent Robots and Systems (IROS 2014), pp. 779-784, 2014.

20. R. Bostelman, T. Hong, S. Legowik, “Mobile Robot and Mobile Manipulator Research Towards ASTM Standards Development”, SPIE 2016, Baltimore, MD, April 2016.

Dynamic Metrology and ASTM E57.02 Dynamic Measurement Standard

Roger Bostelman[1][2], Tsai Hong[1]
[1]National Institute of Standards and Technology, Engineering Laboratory, Intelligent Systems Division, 100 Bureau Drive, MS8230, Gaithersburg, MD 20899
phone (301) 975-3426, roger.bostelman, tsai.hong@nist.gov
[2]IEM, Le2i, Université de Bourgogne, BP 47870, 21078 Dijon, France

Steven Legowik
Robotic Research, LLC
555 Quince Orchard Rd #300,
Gaithersburg, MD 20878
(240) 631-0008
legowik@roboticresearch.com

Mili Shah
Dept. of Mathematics and Statistics,
Loyola University Maryland
4501 N Charles St, Baltimore, MD 21210
(410) 617-2724
mishah@loyola.edu

Word Count: 3169
Number of Images Submitted: 15

Abstract

Optical tracking systems[1] are used in a wide range of fields. The market for optical tracking systems has dramatically increased over the past several years to $1.2B revenue in 2014. This paper describes the new ASTM E3064 Standard test method procedures for optical tracking systems and will outline the theoretical basis for the analysis of the data from these systems. The paper will also verify the performance of an example 12 camera optical tracking system using these standard procedures and related analysis. An artifact, developed at the National Institute of Standards and Technology, was verified by a coordinate measurement machine and then used in two experiments to verify the test method. This and other in-depth papers are intended to be base references for ASTM E3064.

Keywords: optical tracking, coordinate measurement machine, ASTM E3064 standard, reproducible performance, test methods, artifact

1 Introduction

Optical tracking systems measure the three-dimensional, static and dynamic position and orientation of multiple markers attached to objects within a measurement space. Optical tracking systems are used in a wide range of fields including: neuroscience[i], biomechanics[ii], robotics[iii], and automotive[iv] assembly. The market for optical tracking systems has dramatically increased over the past several years to $1.2B revenue in 2014 with annual growth of nearly 53% from 2009 to 2014.[v, vi, vii] Potential users of optical tracking systems often have difficulty comparing systems because of the lack of standard performance metrics and test methods, and therefore must rely on vendor claims regarding the system's performance, capabilities, and suitability for a particular application. The ASTM International Committee E57 on 3D Imaging Systems' subcommittee on test methods addressed the static performance measurement of optical tracking systems[viii]. Recently, the ASTM E57.02 subcommittee task group has developed a new standard test method, "ASTM E3064 Standard Test Method for Evaluating the Performance of Optical Tracking Systems that Measure Six Degrees of Freedom (6DOF) Pose"[ix]. The new test method presents metrics and procedures for measuring, analyzing, and reporting the errors and deviations of dynamic optical tracking

[1] Disclaimer: NIST does not endorse products discussed within this paper nor manufacturers of these products. Products mentioned are for information purposes only and are not expressed as an endorsement for them or their manufacturer.

systems. An artifact, developed at the National Institute of Standards and Technology (NIST) and shown in Figure 1 a - top, was first used to measure a multi-camera system and then expanded by the ASTM E57.02 task group to apply to all types of optical tracking systems. Figure 1 a – top shows an artifact that is used for systems that operate based on active or retroreflective markers and Figure 1 – bottom shows an artifact that can be used for systems that use geometric features as markers. The artifact description in the standard allows for a variety of markers to fit the optical tracking system's measurement method. The end markers are measured relative to one another in each right and left cluster on the bar and combined through mathematical analysis to output the resulting bar length throughout the measurement space.

This proposed standard provides a common set of metrics and a test procedure for evaluating the performance of optical tracking systems and may help to drive improvements and innovations. The standard will also allow users to assess and compare the performance of a candidate optical tracking system and to determine if the measured performance results are within the specifications with regard to the application requirements.

This paper describes the new ASTM E3064 Standard test method procedures for optical tracking systems and will outline the theoretical basis for the analysis of the data from these systems. The paper will also verify the performance of an example, 12 camera optical tracking system. These experiments were conducted using the standard procedures and the analysis method using the artifact shown in Figure 1a (top), which was measured using a coordinate measurement machine (CMM). A second method provided in the standard, not part of this paper, allows the measurement results to be used without prior knowledge of artifact measurement from a CMM or other similar machine. This and other in-depth papers are expected to be the base references for ASTM E57.02.

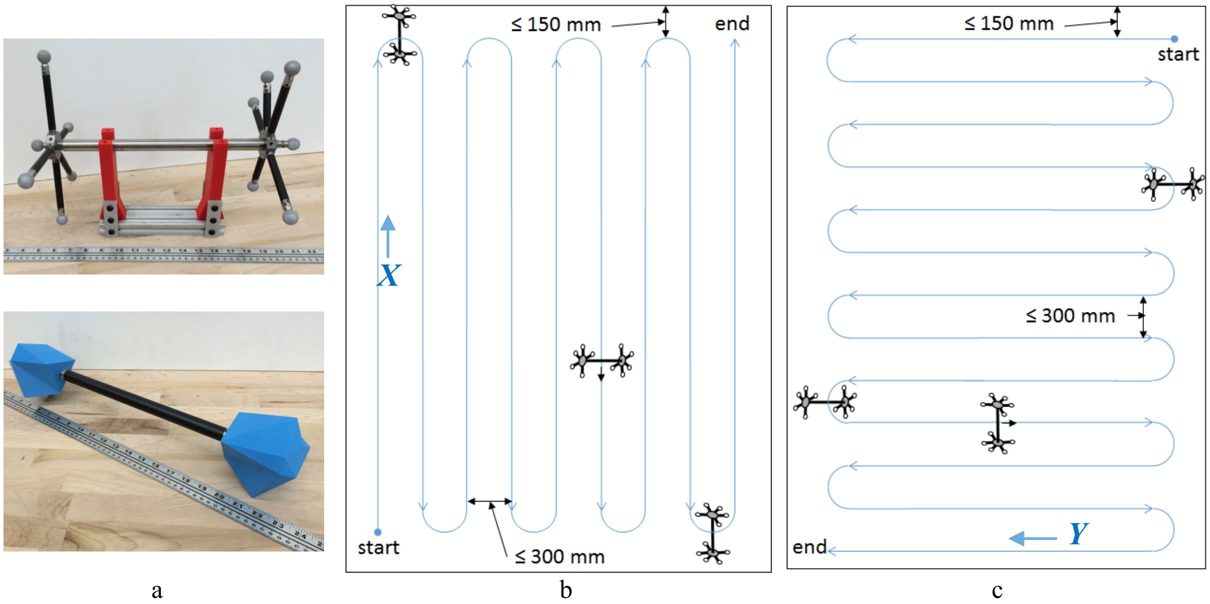


Figure 1 – (a) Artifacts to measure optical tracking system performance. (b) Forward-back (aligned with the X axis) and (c) side-to-side (aligned with the Y axis) paths and dimensions for moving the artifact in a test space. Reprinted, with permission from ASTM E3064-16 Standard Test Method for Evaluating the Performance of Optical Tracking Systems that Measure Six Degrees of Freedom (6DOF) Pose, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428.

2 Metrics and Test Method

ASTM E3064 provides statistically-based performance metrics and a test procedure to evaluate the dynamic performance of optical tracking systems. Measurements from optical tracking systems include inherent positional and orientation angle errors relative to fixed optical measurement components. Metrics are therefore the static and dynamic position and orientation of tracked objects. Beyond the scope of this paper are metrics that are currently being researched which include system latency and maximum dynamic measurement capability.

The test procedure outlined in E3064 measures the relative pose between two sets of markers that are rigidly attached to the ends of a metrology bar as shown in Figure 1a. The relative pose is then decomposed into positional and angular components and measurement errors are calculated by comparing results to a known metrology bar length of the artifact.

The artifact includes a 300 mm long metrology bar with markers rigidly attached to each end. The bar is called a 'metrology bar' since it has stiffness and thermal expansion characteristics to allow deflection of less than or equal to 0.01 mm. Example metrology bars are made of carbon fiber or titanium that meet the mandatory minimal deflection characteristic. One form of artifact includes two clusters of passive, reflective, spherical (see Figure 1a top) or active, light-emitting-diode (LED) markers located at the ends of the metrology bar. Another form uses reduced pose ambiguity cuboctahedron[x] (see Figure 1a bottom) markers. Both types of markers must be contained within hemispherical volumes of 100 mm maximum radius from the ends of the bar.

The basic procedure for determining the pose measurement error of an optical tracking system first includes rough (hand-held) alignment of the X and Y axes (Figure 1) and Z axis (aligned with the vertical axis) within the test volume to be measured. The options for the test volume are: (1) 3000 mm long x 2000 mm wide x 2000 mm high, (2) 6000 mm long x 4000 mm wide x 2000 mm high, and (3) 12000 mm long x 8000 mm wide x 2000 mm high.

The optical tracking system tracks the metrology bar as it is moved throughout the test volume along the two patterns shown in Figure 1b and Figure 1c for three trials. The metrology bar in each trial corresponds to one of the three orientations shown in Figure 2. The centroid of the metrology bar is to remain at approximately 1 m above the test volume floor and should be moved at approximately the walking speed of 1.2 m/s ± 0.7 m/s. The metrology bar length is used as a guideline for determining both the distance between the boundary lines and the limits of the test volume. The data from these three trials are then combined into one data set.

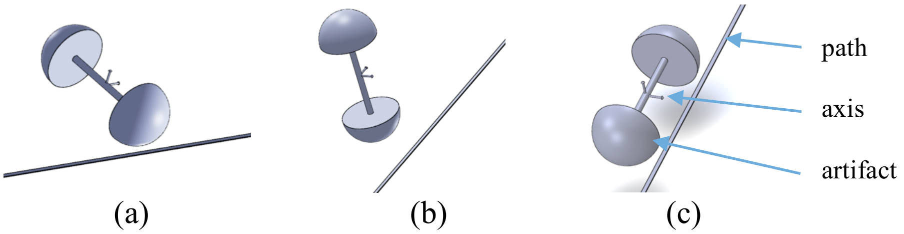


Figure 2: The artifact (shown with axes on the bar centroid) orientations with respect to the path: (a) perpendicular to the path segments in the plane of motion, (b) perpendicular to the path segments and normal to the plane of motion, and (c) in-line with the path segments in the plane of motion. The artifact shown in Figure 1 ((a) and (b)) is oriented with respect to the path as in (a) perpendicular to the path segments in the plane of motion. This caption includes descriptions directly from E3064. Reprinted, with permission from ASTM E3064-16 Standard Test Method for Evaluating the Performance of Optical Tracking Systems that Measure Six Degrees of Freedom (6DOF) Pose, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428.

The data gathered from the optical tracking system (OTS) consist of the 6DOF pose of the left and right ends of the artifact at time *t* represented as the homogeneous matrices

$$ {}_{OTS}\hat{H}_{Left}(t) = \begin{bmatrix} \hat{R}_{Left}(t) & \hat{T}_{Left}(t) \\ 0 & 1 \end{bmatrix} \text{ and } {}_{OTS}\hat{H}_{Right}(t) = \begin{bmatrix} \hat{R}_{Right}(t) & \hat{T}_{Right}(t) \\ 0 & 1 \end{bmatrix}. $$

Then the relative pose between the left and right markers is defined as

$$ {}_{Left}\hat{H}_{Right}(t) = {}_{OTS}\hat{H}^{-1}_{Left}\,{}_{OTS}\hat{H}_{Right} = \begin{bmatrix} \hat{R}_{Left}(t) & \hat{T}_{Left}(t) \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} \hat{R}_{Right}(t) & \hat{T}_{Right}(t) \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \hat{R}(t) & \hat{T}(t) \\ 0 & 1 \end{bmatrix}, $$

where $\hat{R}(t)$ is the 3x3 rotation matrix describing the relative orientation between the left and right markers and $\hat{T}(t)$ is the 3x1 vector describing the relative translation between the left and right markers. The angle of rotation can then be described as

$$\hat{\theta}(t) = 2 * \operatorname{asin}(\sqrt{\hat{q}_x^2(t) + \hat{q}_y^2(t) + \hat{q}_z^2(t)}\ ),$$

where $\left(\hat{q}_w(t), \hat{q}_x(t), \hat{q}_y(t), \hat{q}_z(t)\right)^T$ is the unit quaternion representation of $\hat{R}(t)$ and $\hat{q}_w(t)$is the scalar component of the quaternion.

If the relative pose between the left and right markers has been measured by a reference system and represented as

$$_{Left}H_{Right} = \begin{bmatrix} R & T \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} I & T \\ 0 & 1 \end{bmatrix},$$

then the position error at time *t* can be defined as

$$e_{p(t)} = \left\|\hat{T}(t)\right\| - \|T\|,$$

and the orientation error at time *t* can be defined as

$$e_{o(t)} = \hat{\theta}(t) - 0 = \hat{\theta}(t).$$

Statistics on these errors include:

Root Mean Square	RMS	$\sqrt{\frac{1}{N}\sum_{t=1}^{N} e_t^2}$
Maximum Error	e_{max}	$\max(\lvert e_1\rvert, \lvert e_2\rvert, \dots, \lvert e_N\rvert)$
Percentile Error	$E(p)$	$\begin{cases} E_k + d(E_{k+1} - E_k), & 0 < k < N \\ E_1, & k = 0 \\ E_N & k \geq N \end{cases}$

Here, e_t denotes either the positional error $e_{p(t)}$ or the orientation error $e_{o(t)}$. In addition, the percentile error *E(p)* on the ordered set $\{E_1, E_2, \dots, E_N\}$ is constructed from rearranging the set of errors $\{\lvert e_1\rvert, \lvert e_2\rvert, \dots, \lvert e_N\rvert\}$ by increasing value. Moreover,

$$\frac{p}{100}(N + 1) = k + d,$$

where *k* is an integer and $0 \leq d < 1$. The specific percentile errors reported are *E(99.7), E(95),* and *E(50).*

3 Experiments

Experiments were performed (A) to test the motion of optical tracking system camera mounts and (B) to test the ASTM E3064 standard test method. Optical tracking system camera mounting is critical to providing the best system calibration possible. If there is camera motion, the system measurement will provide less certainty than with fixed camera mounts. Hence, a measurement of camera motion is useful to determine how much motion the reference frame including all cameras provides. The authors measured the motion of two cameras mounted in worst-case locations for the reader to further understand this concept.

For experiment A, two optical tracking system camera mounts were tracked for 24 hours each using a laser tracker with an uncertainty of approximately 10 µm[xi]. Magnetic retro reflector mounts were glued to the two camera mounts located near the center of the longest walls of the rectangular laboratory. The laboratory, shown in Figure 3, has 12 optical tracking system cameras mounted at a height of 4.3 m on 6.7 m high perimeter walls. The laser tracker was programmed to take a data point each second for a total of 86,400 data points. The inside laboratory environment remained at a relatively constant room temperature and humidity. However, during the outside wall motion measurement, the outside temperature changed by approximately 30° F between day and night. The day was rainy, cloudy with no sun and a high of approximately 55° F. Optical tracking system calibration and experiment B were not, however, performed during the same day as experiment A since the laser tracker beam would have been obstructed during calibration and the experiment.

Before experiment B, an optical tracking system calibration routine was performed. The routine included ensuring that extraneous reflectors were covered. These included a set of thirteen reflectors, mounted on the perimeter walls for automatic guided vehicle (AGV) navigation, were covered. The AGV with onboard robot arm, including reflective markers detectable by the optical tracking system, were also covered with a large sheet of black plastic. Also, the floor was covered with black plastic due to reflections onto the floor tile caused by infrared light emitting diodes surrounding each camera. When the reflections were minimized, the tracking system was calibrated by waving the manufacturer's calibration wand throughout the work volume until the system termed the calibration as 'exceptional' meaning a high confidence in the calibration.

Experiment B used the artifact shown in Figure 1a top. The paths shown in Figure 1b were then walked at an estimated speed of 1.2 m/s ± 0.7 m/s (as noted by the standard) over an area of approximately13 m by 6 m while the optical tracking system tracked the artifact motion. The artifact was held at a height of approximately 2 m and oriented as in the Figure 2a. This test area is similar to the third test volume described in Section 2: Metrics and Test Method. After both X and Y paths were walked with the artifact in the first artifact orientation, the experiment was repeated with the artifact held in the orientations shown in Figure 2b and Figure 2c. The data were then combined into a single data set, as required in the standard, and analyzed. The test method was then repeated for a second trial on another day after recalibration to ensure that experiment B was properly performed and that the data retrieved were similar to the first day experiment B. The total experiment B took roughly 12 minutes.

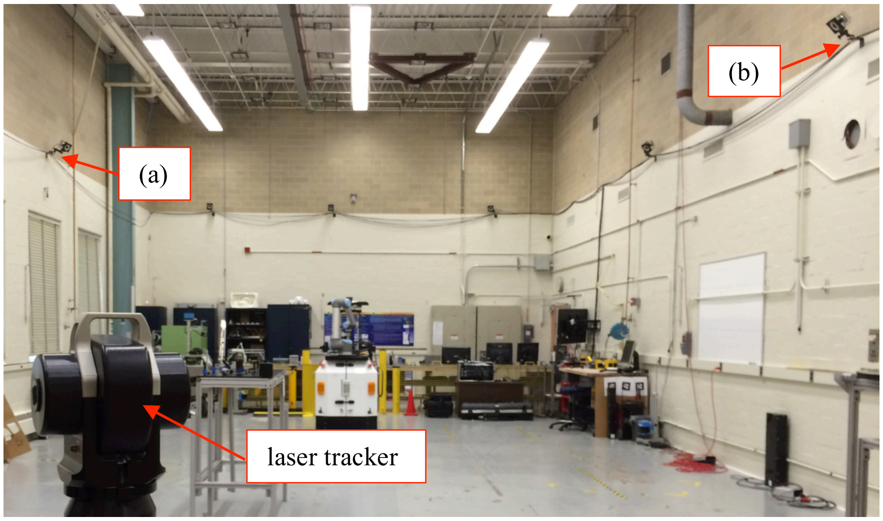


Figure 3. Laser tracker measuring a laboratory, outside-wall, mount (a) that supports an optical tracking system camera. On the right is the (b) inside-wall mount that was measured.

4 Experimental Results

For experiment A, the laser tracker provided results over 24 hours where, as expected, the inside wall moved much less than the outside wall. The data is shown in Figure 4 for both wall measurements.

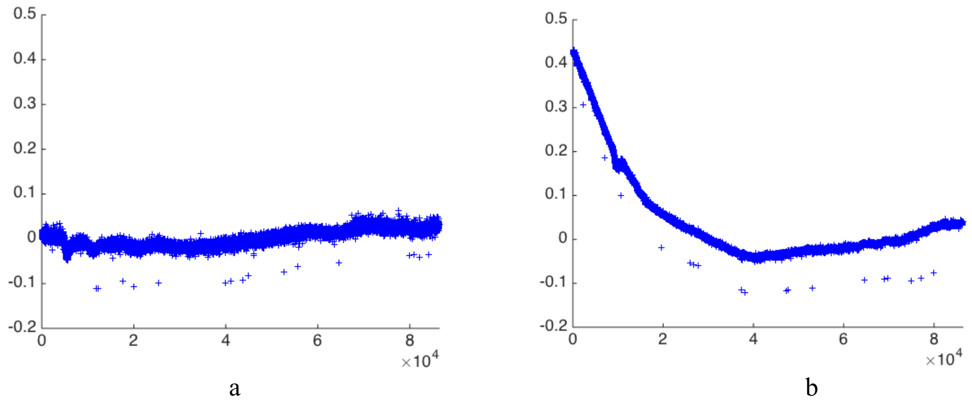


Figure 4. Laser tracker data from measurement of two camera mounts supporting optical tracking system cameras inside the laboratory on (a) an inside block wall and (b) an outside block wall. The horizontal axis is in sample points and the vertical axis is in mm.

For example, disregarding outliers, wall motion data spanned between approximately + 0.04 mm and - 0.05 mm for the inside wall and between approximately + 0.43 mm and - 0.05 mm maximum for the outside wall. Outside wall measurement began at 2 PM. Most motion of the outside wall was between 2 PM and 2 AM as shown in the left half of Figure 4 (b). The optical tracking data captured for experiment B and for calibration were collected over a period of only approximately 30 min. each. Therefore, the motion of the walls during these periods was approximately 0.02 mm for the inside wall and 0.04 for the outside wall.

A sample data plot of the X and Y tracked paths is shown in Figure 5. The plot is of data collected from walking with the artifact in the vertical orientation (Figure 2b) during the second trial. Experiment B results are shown in Table 1 for the two trials including analyzed data from both the artifact bar length and angle between artifact end-markers. The root mean square deviation (RMSD) shows approximately 0.5 mm length difference from the actual 300 mm length and approximately 0.34° difference from 0° actual angle. The maximum error, 50th percentile, 95th percentile, and 99.7th percentile length and angle results are also shown.

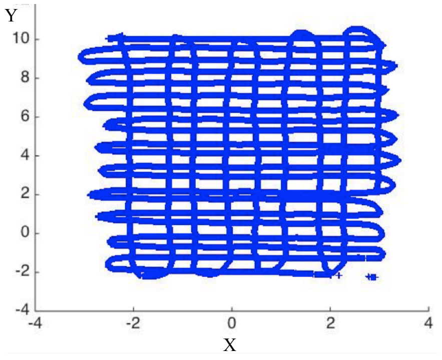
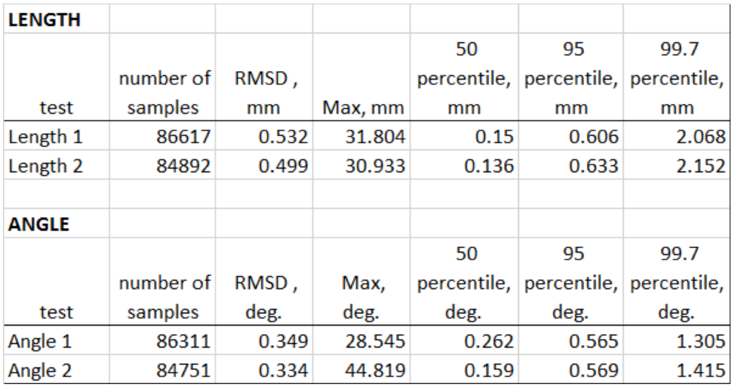


Figure 5. Sample data plot of the X and Y tracked paths of the artifact center.



LENGTH						
test	number of samples	RMSD , mm	Max, mm	50 percentile, mm	95 percentile, mm	99.7 percentile, mm
Length 1	86617	0.532	31.804	0.15	0.606	2.068
Length 2	84892	0.499	30.933	0.136	0.633	2.152
ANGLE						
test	number of samples	RMSD , deg.	Max, deg.	50 percentile, deg.	95 percentile, deg.	99.7 percentile, deg.
Angle 1	86311	0.349	28.545	0.262	0.565	1.305
Angle 2	84751	0.334	44.819	0.159	0.569	1.415

Table 1. Experimental results from the two trials.

The percentile error is listed in the ASTM E3064 standard, as opposed to the standard deviation, since the data distribution may not be Gaussian. Histogram plots of the 99.7th percentile distribution are shown in Figure 6. As shown, the length data is relatively evenly distributed whereas the angle data is shifted positive.

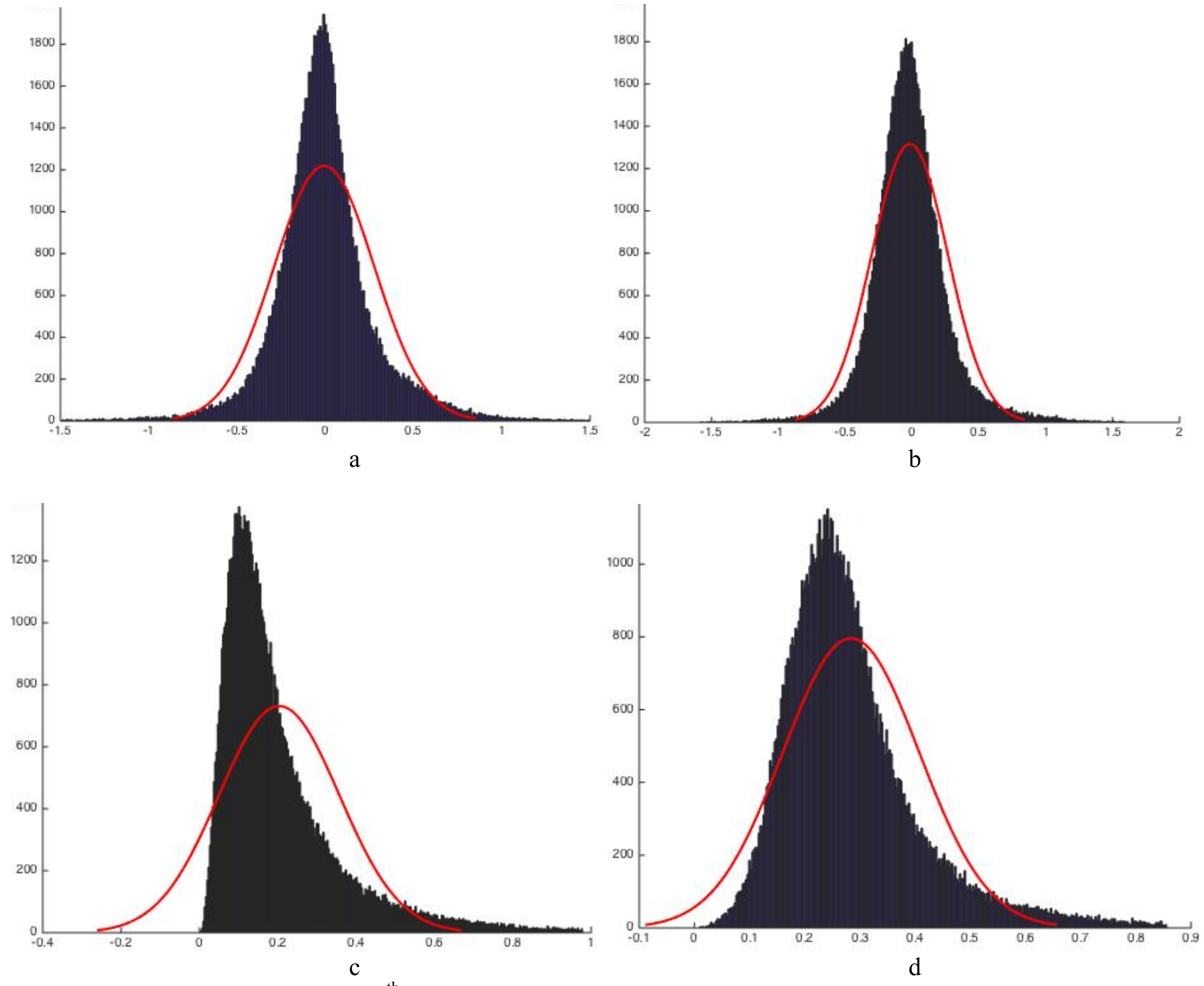


Figure 6. Histogram plots of the 99.7th percentile data shown in Table 1 for (a) Length from Trial 1, (b) Length from Trial 2, (c) Angle from Trial 1 and (d) Angle from Trial 2. The Gaussian distribution (red) is shown for comparison.

5 Conclusions

Optical tracking systems are used in a wide range of fields and have dramatically grown in market share over the past several years. As such, a team of optical tracking system manufacturers, users, and researchers who were part of an ASTM E57.02 task group developed a standard test method (ASTM E3064). Towards completion of the standard, the test method procedures within the standard were tested in two experiments described in this paper. The theoretical basis for data analysis was also described in this paper followed by analysis of the experimental data using this method. The paper verified the performance of an example 12 camera optical tracking system with an artifact, developed at NIST and measured previously using a coordinate measurement machine. Experimental results showed that the test method provides an RMSD of approximately 0.5 mm length difference from the actual 300 mm length and approximately 0.34° difference from 0° actual angle. Also, the use of percentiles versus standard deviation was verified through histogram plots resulting in offset from the mean. To ensure that the optical tracking system was mounted and calibrated properly, a high-accuracy laser tracker was used to verify that the system camera mounts only slightly moved (i.e., approximately 0.02 mm for the inside wall and 0.04 for the outside wall) relative to the artifact RMSD results. Additionally, a system calibration was performed prior to each experiment. Future optical tracking system standard efforts will be focused on system latency and perhaps other dynamic measurement performance characteristics.

Acknowledgements

The authors would like to thank the hard work and dedication of the ASTM E57.02 Subcommittee task group for developing the E3064 standard. We also thank Dan Sawyer and his team from the NIST Dimensional Metrology Group for helping to develop and test the artifact.

References

[i] Warren WH, Kay BA, Zosh WD, Duchon AP, Sahuc S. Optic flow is used to control human walking. Nature neuroscience. 2001 Feb 1;4(2):213-6.

[ii] OptiTrack for Movement Sciences, http://www.optitrack.com/motion-capture-movement-sciences/, 2016.

[iii] Bostelman, R., Falco, J., Shah, M. and Hong, T., "Dynamic Metrology Performance Measurement of a Six Degree-of-Freedom Tracking System Used in Smart Manufacturing", ASTM International STP1594: *Autonomous Industrial Vehicles: From the Laboratory to the Factory Floor*, R. Bostelman and E. Messina, Eds., Ch. 7, pp. 91-105, 2016.

[iv] Shackleford, W., Cheok, G., Hong, T-H, Saidi, K., and Shneier, M., "Performance Evaluation of Human Detection Systems for Robot Safety," Journal of Intelligent & Robotic Systems, Jan. 2016.

[v] "Motion Capture Software Developers in the US: Market Research Report," IBIS World 2014.

[vi] Moeslund, T. B., Hilton, A, and Krüger, V.,"A survey of advances in vision-based human motion capture and analysis," Computer Vision and Image Understanding, vol. 104, no. 2, 2006.

[vii] Field, M., Stirling, D., Naghdy, F., Pan, Z., "Motion Capture in Robotics Review," 6th IEEE International Conference on Control &Automation, New Zealand, Dec 2009.

[viii] ASTM E2919-14, http://www.astm.org/Standards/E2919.htm.

[ix] ASTM E3064 Standard Test Method for Evaluating the Performance of Optical Tracking Systems that Measure Six Degrees of Freedom (6DOF) Pose, www.astm.org, 2016.

[x] English, C., Okouneva, G., Saint-Cyr, P., Choudlhuri, A., Luu, T., "Real-Time Dynamic Pose Estimation Systems in Space: Lessons Learned for System Design and Performance Evaluation," International Journal of Intelligent Control and Systems (IJICS), vol. 16, no. 2, 2011.

[xi] Burge, James H., Peng Su, Chunyu Zhao, and Tom Zobrist. "Use of a commercial laser tracker for optical alignment." In Optical Engineering+ Applications, pp. 66760E-66760E. International Society for Optics and Photonics, 2007.

Intelligence Level Performance Standards Research for Autonomous Vehicles

Roger B. Bostelman, Tsai H. Hong, and Elena Messina

Abstract— **United States and European safety standards have evolved to protect workers near Automatic Guided Vehicles (AGV's). However, performance standards for AGV's and mobile robots have only recently begun development. Lessons can be learned from research and standards efforts for mobile robots applied to emergency response and military applications. Research challenges, tests and evaluations, and programs to develop higher intelligence levels for vehicles can also used to guide industrial AGV developments towards more adaptable and intelligent systems. These other efforts also provide useful standards development criteria for AGV performance test methods. Current standards areas being considered for AGVs are for docking, navigation, obstacle avoidance, and the ground truth systems that measure performance. This paper provides a look to the future with standards developments in both the performance of vehicles and the dynamic perception systems that measure intelligent vehicle performance**.

I. Introduction

Automatic Guided Vehicles (AGV's) have typically been used for industrial material handling since the 1950's. Since then, U.S. [1] and European [2] AGV safety standards have evolved to protect nearby workers. These standards have minimal test methods to describe how manufacturers and users are to perform AGV safety measurements, resulting in potential measurement differences across the industry. For example, American National Standards Institute/Industrial Truck Safety Development Foundation (ANSI/ITSDF) B56.5:2012 provides new language to generically handle a situation when an object suddenly appears within the AGV stop region. The stop region is the area surrounding the AGV in which the non-contact safety sensor detects obstacles and stops the vehicle. The manufacturer must now prove that when the AGV detects an object closer than its stopping distance, although collision with the object is perhaps imminent, the AGV demonstrates a reduction in kinetic energy. However, there is no description of how manufacturers measure this situation, resulting in different measurement results across manufacturers. One test method was researched to handle this situation and is described in [3].

Recently AGV and mobile robot performance standards developments have begun to limit measurement method differences. Initial developments began with a review of other research and standards efforts for mobile robots as applied to emergency response and military applications [4]. This reference also discusses research challenges, test and evaluations, and intelligent systems development programs that can support advancement of industrial AGVs towards attaining greater levels of intelligence. These other efforts also provide useful standards development criteria for AGV performance test methods. Experiences and results in advanced mobility and intelligence for robotics will be essential for AGV manufacturers and users to fully understand capabilities and specific applications of their autonomous vehicle systems.

Performance test methods for docking, navigation, (see Figure 1) [5], and terminology standard work items have been initiated under the new ASTM Committee F45 on Driverless Automatic Guided Industrial Vehicles performance standard [6]. Standards for autonomous industrial vehicle obstacle avoidance and protection, based on past research [7], communication and integration, and environmental impacts are also being considered.

This paper will specifically discuss measurement of: vehicle navigation (e.g., commanded vs. actual AGV path-following deviation), vehicle docking (e.g., AGV stop point positioning vs. known facility points), and obstacle detection and avoidance of standard test pieces (e.g., comparison of real-time AGV path-planning and new path following vs. commanded path) towards smart manufacturing applications, such as assembly and unstructured environment navigation. Additionally, this paper will discuss a new ASTM Committee on 3D Imaging Systems E57.02 [8] standard work item for six degree-of-freedom (DOF) optical measurement of dynamic systems (see Figure 2), which advances the existing static 6 DOF standard [9]. The new standard is expected to be a critical component of performance measurement for current and future robotic systems that rely on advanced perception systems.

II. Performance Standards Thrusts

AGV navigation, docking, and obstacle detection and avoidance tests were conducted in support of future performance standard test methods and are described in this section. In some instances, typical industry practices were evaluated as well as the improved AGV performance tests.

R. V. Bostelman is with the National Institute of Standards and Technology, Gaithersburg, MD 20899, USA and with the IEM, Le2i, Université de Bourgogne, BP 47870, 21078 Dijon, France (phone: 301-975-3426; fax: 301-990-9688; e-mail: roger.bostelman@nist.gov).

T. H. Hong, is with the National Institute of Standards and Technology, Gaithersburg, MD 20899, USA (phone: 301-975-3444; fax: 301-990-9688; e-mail: tsai.hong@nist.gov).

E. Messina is with the National Institute of Standards and Technology, Gaithersburg, MD 20899, USA (phone: 301-975-3510; fax: 301-990-9688; e-mail: elena.messina@nist.gov).

A. Vehicle Navigation

The most basic functions of mobile robots and AGV's are navigation to and docking with equipment in the workspace. However, the description of how well the vehicle navigates (i.e., commanded vs. actual AGV path-following deviation) has certain ambiguities. For example, navigation implies that the vehicle measures its current position, plans a route to another location, and moves from the current location to planned location upon command. Most vehicle manufacturers don't provide specifications for how uncertain the navigation performance is (i.e., the error bounds on position or velocity), other than perhaps radius of vehicle turns, maximum velocity, and maximum acceleration. The vehicle velocity sets limits on the allowable turn radius for particular vehicles. Some controllers [10], if not all, will not allow high velocities on relatively small radii to prevent unsafe vehicle conditions. These limitations are not typically specified by AGV manufactures, causing AGV users difficulty in planning how many vehicles they may require for moving their products within the facility to maintain a desired throughput.

Industrial vehicles may eventually become uncalibrated through regular use. An uncalibrated vehicle does not follow a commanded path or stop/dock at a commanded point with minimal relative uncertainty (standard deviation of measured vs. ground truth) as does a calibrated vehicle. To correct this, vehicle manufacturers have calibration procedures for their vehicles, although these procedures can be tedious, time-consuming, and may not be appropriate for all vehicles. For example, calibration of Ackerman steered vs. 'crab' steered (sometimes called quad) vehicles have different calibration procedures. It is not always clear what will happen when a vehicle is uncalibrated nor when the vehicle becomes uncalibrated. The effects of calibration on vehicle control and uncertainty are typically not specified either. There is also typically no specification describing how far from the commanded path a vehicle navigates. This may be important to users who have tight tolerance AGV paths (e.g., paths between infrastructure) that must be followed. A test can be developed to uncover the effects of uncalibrated vs. calibrated vehicle navigation performance when commanded to move along a path, as shown as a dashed line in the example in Figure 1. Should objects be near the vehicle path, such as walls or obstacles, depicted in Figure 1 as bordering lines along the path, the vehicle may stop, slow, or worse, collide with the boundary object. A user would then be required to provide additional, perhaps unnecessary space for one manufacturers' vehicle and not for another. How the vehicle handles (slow, stop, etc.) the event is also ambiguous. For example, some, but not all vehicles are equipped with obstacle detection based on non-contacting sensors that provide detection beyond the physical vehicle footprint.

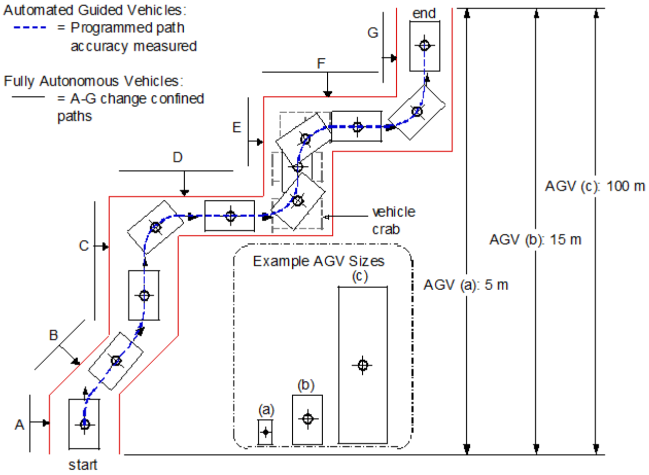

Automated Guided Vehicles:
= Programmed path accuracy measured
Fully Autonomous Vehicles:
= A-G change confined paths
A
B
C
D
E
F
G
end
start
vehicle crab
Example AGV Sizes
(a)
(b)
(c)
AGV (c): 100 m
AGV (b): 15 m
AGV (a): 5 m

Figure 1. Example reconfigurable apparatus for navigation tests for various AGV sizes.

To address AGV navigation uncertainty, with an eye towards a potential test method for all automatic industrial vehicles, tests were executed, both with an AGV prior to and after being calibrated. The uncalibrated AGV test is similar to typical industry methods since not all AGVs can be frequently calibrated. An uncalibrated AGV was moved along a straight line path between two commanded points in an open area and spaced approximately 5 m apart [5]. Figure 2 shows the results amplified in the X direction 100 times to exaggerate vehicle performance. In the figure, the blue line is the commanded path between points 1 and 2. The green dots to the right and left of the line are uncalibrated AGV controller-traced position data moving forward and reverse, respectively, between the points. The red dots are ground truth of the navigating AGV between points using an optical tracking system. This experiment demonstrated one AGV navigation performance measurement method using a precision (0.2 mm standard deviation) six degree-of-freedom (DOF), optical measurement system as a ground truth comparison to the onboard vehicle tracking system. Path deviation was approximately 20 cm maximum. The AGV was then calibrated using the manufacturer's method.

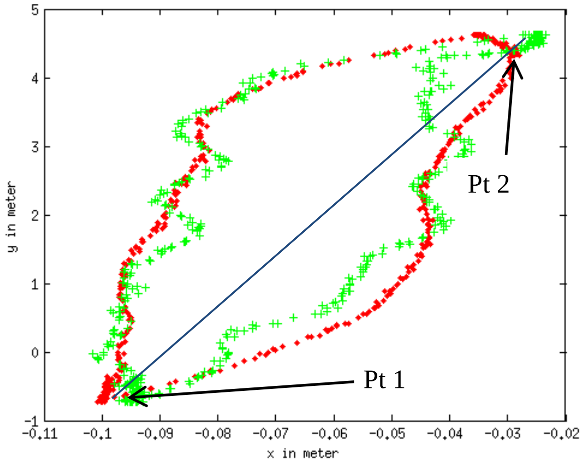


Figure 2. Ground Truth (red) and AGV (green) data of the straight line path tests. Scales for X and Y axes are in meters where the X axis shows only -0.11 to -0.02 range to clearly show the AGV performance as compared to Ground Truth measurement. The blue line represents the commanded path from pt 1 to pt 2 and back.

Another test setup was tried, with an eye towards a relatively less expensive test method that will allow all AGV systems to be measured, ideally, with an independent measurement method that doesn't use AGV controller tracking, yet captures the full AGV configuration (i.e., including safety sensing). The AGV was commanded to drive back and forth between temporary barriers, along a straight line defined by commanded points spaced approximately 10 m apart. The goal of the experiment was to measure the AGV deviation from the commanded path. A critical AGV navigation performance area is also deviation from the commanded path after turns so a 90° turn was added to the end of the straight path beyond the barriers to measure the vehicle navigation uncertainty when moving from/to a straight path to/from a turn. Figure 3 shows the test setup and Figure 4 shows (a) a B56.5 test piece being used to define the safety laser stop field edges, (b) the barriers and lines to which barriers are moved between trials, and (c) the AGV emergency-stopped upon detection of the barriers. The safety laser, stop field edges were marked on the floor, as a ground truth, zero-tolerance spacing that the vehicle can navigate, when the vehicle was at position 1 and again at position 3, shown in Figure 3, for both left and right vehicle sides. The barrier position lines were measured from the edge line using a ruler and marked at 2 cm increments from the edge up to 10 cm away from the edge line. Smaller spacing between lines (e.g., 1 cm) could also be used for finer uncertainty measurement. For each test trial, the barriers were moved towards the AGV to the next line beginning at 10 cm for trial 1, 8 cm for trial 2, and so forth until the navigating vehicle detected a barrier, and emergency-stopped the AGV, thus completing the test run.

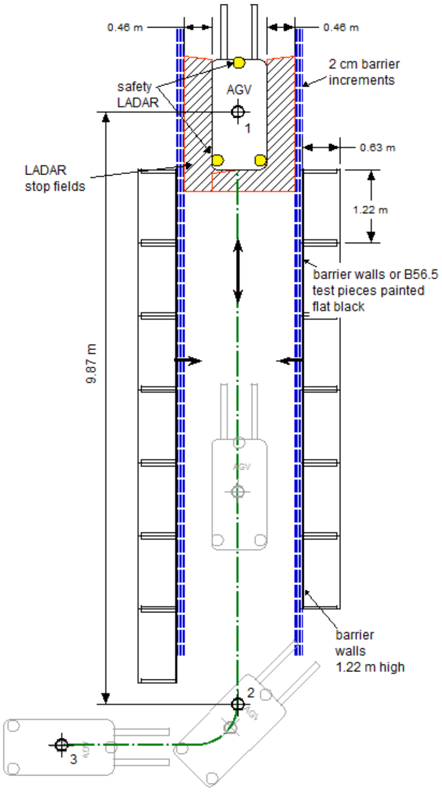


Figure 3. AGV navigation test setup.

A series of eight trials were completed with nearly all trials including three or more runs each to demonstrate the navigation test method concept. Ten or more runs are ideal for statistical analysis. The optical measurement system mentioned earlier was used as an experimental ground truth (GT) to measure the barrier and vehicle position during experiments to further understand the test method and vehicle performance. The barriers and AGV were marked with spherical reflectors (visible in Figure 4 (a, b, and c) detectable from the GT system. Figure 5 presents GT data plotted for navigation tests showing ground truth data of: (a) test 8 vehicle path and emergency stopped vehicle (red circle) when a wall was detected, (b) test 1 path, and (c) test 1 path data from (b) zoomed in to show data points of three runs.

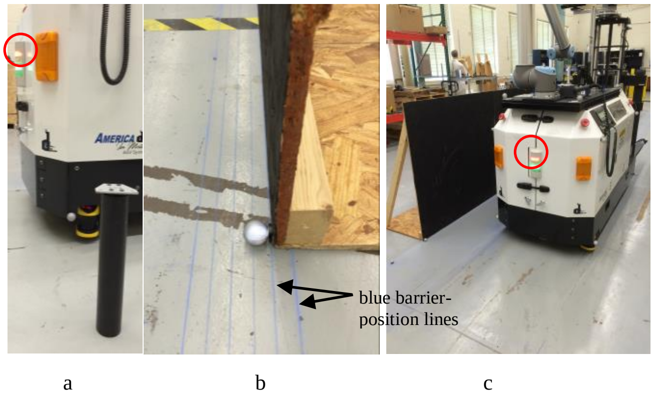


Figure 4. (a) B56.5 test piece (black cylinder) used to define safety laser edge (note red emergency stop light (within the red circles) is on), (b) barrier (black) painted wood panel, blue lines spaced at 2 cm, and spherical reflector from ground truth system, (c) AGV emergency stopped, as noted by the red light, upon detection of barriers during a test.

Experimental results from the barriers demonstrated a path uncertainty of between 6 cm and 8 cm maximum when the vehicle detected the boundaries at nearly the center of the straight line path and when moving at either 0.25 m/s or 0.50 m/s. The navigation test method using barriers is simple and cost-effective for manufacturers and users to employ, as compared to the higher accuracy, but more expensive ground truth visual tracking system used for test method development. A simple straight line with one turn was tested. However, more complex test configurations, such as shown in Figure 1, could be set up using B56.5 test pieces instead of larger, physical barriers as were used in this research.

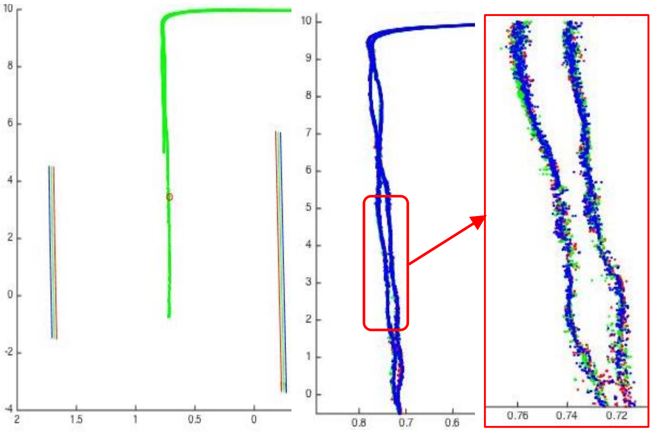


Figure 5. Example graphical results of navigation tests showing ground truth data of: (a) test 8 vehicle path and emergency stopped vehicle (red circle)

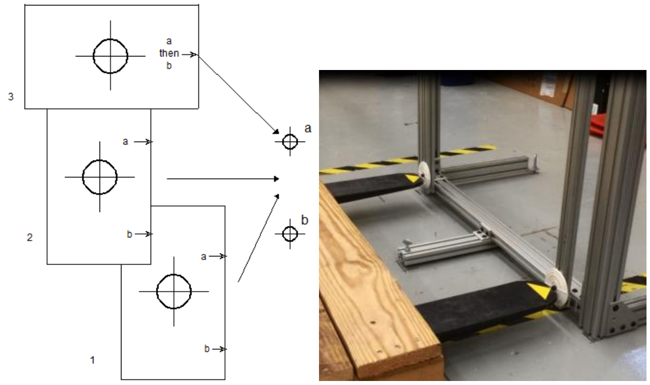
when a wall was detected, (b) test 1 path, and (c) test 1 path data from (b) zoomed in to show (red, green and blue) data points from three runs.

A working document that addresses quantifying vehicle navigation uncertainty is being developed as an initial step towards a performance standard for ASTM F45.02 subcommittee on Docking and Navigation. Based on consensus of the task group developing this standard, as was tested at NIST, the simple path-bounding test method using temporary reconfigurable barriers made from readily-available, off-the-shelf materials is being proposed.

B. *Vehicle Docking*

Vehicle docking is another common application of mobile robots and AGVs. Unit load (tray, pallet, or cabinet carrying), tugger (cart pulling), and fork/clamp (pallet or box load/unloading) are typical industrial style vehicles that require different docking uncertainties. For example, a unit load vehicle that places/retrieves platters during wafer manufacturing would no doubt require less uncertainty than a fork style vehicle that places/retrieves pallets. As robotics advances, current and potential users are requesting mobile manipulators to perform tasks such as unloading trucks. Eventually, it is expected that mobile manipulators will be used for smart manufacturing assembly applications [11, 12].

Similar to navigation, there are no performance measurement test methods that define how manufacturers and users characterize their vehicle's docking capabilities. Figure 6 (a) shows an example method for docking for any style vehicle. A vehicle approaches and makes contact with 'a' and/or 'b' docking points dependent upon the vehicle type. Relative displacement from each of the points would be measured to determine vehicle docking uncertainty. A fork-type AGV is shown docked with a test apparatus in Figure 6 (b). The fork tips are marked with yellow points.



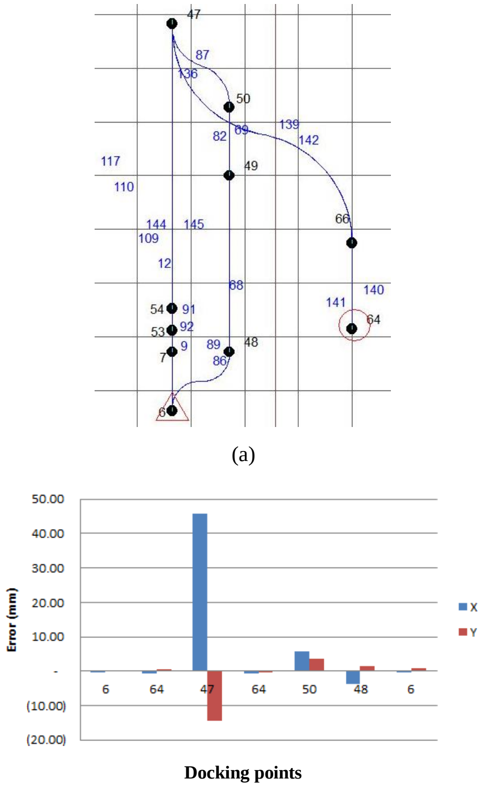
(a) (b)

Figure 6. (a) Example docking test method using various AGVs (e.g., 1 and 2 for AGV unit load tray table docking, 3 for fork and tugger AGV docking). "a" and "b" are fixed points in space (e.g., contact or non-contact sensor locations in space). Approach vectors and sensor point spacing and locations are variable. (b) Fork-type AGV docking with a docking apparatus.

Two experiments were simultaneously performed: AGV docking relative to known facility locations and GT system use for measuring AGV docking. Two different GT measurement systems were used to measure AGV performance: a laser tracking GT with an uncertainty of approximately 10 µm [13] and an optical tracking system with uncertainty of 0.2 mm in position uncertainty and 0.13° in angle uncertainty as measured at NIST. The laser tracker tracks position of a single point, whereas the visual tracking system can track multiple point markers and can computer orientation from them. Both GT systems can measure relatively high-precision displacement between two points, as compared to an AGV docking.

An experiment using an uncalibrated AGV that was programmed to stop at various points yielded an uncertainty range of approximately 1 mm to 50 mm. Figure 7 (a) shows the vehicle paths and Figure 7 (b) shows average errors for five runs at stop or dock points. The vehicle position was measured using a laser tracking GT system which provided high-precision measurement of AGV stop points. [13] However, in several experiments, laser tracker positioning was critical as the laser beam was continuously interrupted by onboard AGV hardware. This prompted a switch to using an optical tracking system for GT measurements.

A 6 DoF optical tracking GT system was used instead to measure AGV docking. Docking was measured again after the AGV was calibrated using the manufacturer's procedures. The AGV approached similar dock locations and after AGV calibration, provided consistent 5 mm uncertainty. Standards development for optical tracking systems is also underway and is discussed in section 2 D, 6 DOF Optical Measurement of Dynamic Systems.



(a)

(b)

Figure7. (a) Commanded paths and stop points and (b) stop point errors of a single AGV point for each location in (a) averaged over 5 runs.

Additional AGV equipment docking experiments were also performed using a mobile manipulator and a reconfigurable mobile manipulator artifact (RMMA) developed at NIST (see Figure 8). [14] The mobile manipulator, with uncalibrated AGV, repeatedly moved next to the artifact from a starting point. Although uncalibrated, the

AGV provided relatively low repeatability uncertainty (e.g., +/-5 mm) although more than 10 mm from the commanded docking points. This manipulator could reach the commanded points on the RMMA even with 10 mm uncertainty in AGV position. The mobile manipulator corrected for the position uncertainty after being taught the actual RMMA locations. At the RMMA, the manipulator, wielding a laser retroreflector, was commanded to move in a spiral pattern to detect 6 mm diameter reflectors. The reflectors provide non-contact alignment detection of the tool point position and orientation. The experiment provided results demonstrating that this relatively inexpensive ground truth measurement method was sufficient for measuring docking accuracy. As the reflector based measurement system is inexpensive compared to the optical tracking-based GT, it may prove ideal for use as a precision vehicle/mobile manipulator docking test method that both manufacturers and users can replicate.

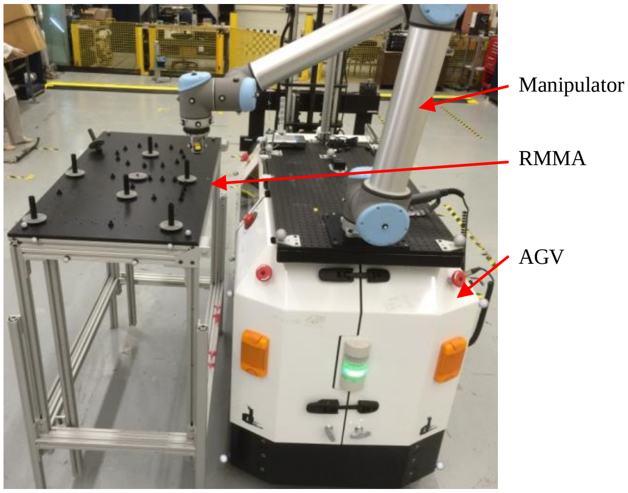


Figure 8. Docking performance measurement of a mobile manipulator with a reconfigurable mobile manipulator artifact (RMMA).

C. Obstacle Detection and Avoidance

Obstacle detection and avoidance (ODA) research is well documented in the literature for mobile robots. However, there are few citations for AGVs perhaps due to the relatively closed nature of commercially available AGV controllers and because ODA is not often implemented on AGVs deployed in large manufacturing facilities. In [5], it was discussed that for large facilities, ODA could occur in ‘buffer zones’ (i.e., zones where AGVs would be allowed to pass other vehicles). For small and medium manufacturing facilities, however, ODA may be necessary due to more limited floor space and less-controlled environments. NIST has developed an algorithm, detailed in [5], and measured the performance of an AGV with added ODA capability. The algorithm is also suitable for navigating an unstructured environment although it is currently limited by the use of facility-mounted (sensors not mounted on the AGV) obstacle detection with obstacle avoidance adapted to an AGV with a controller with limited ability to integrate external algorithms. Figure 9 shows a snapshot of the ODA algorithm planning a path through multiple obstacles.

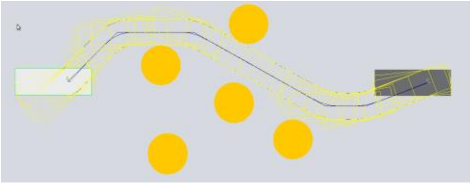


Figure 9. Graphical output of path planner, starting footprint of the AGV is in white, the goal position is a dark grey rectangle. Yellow rectangles show the area swept out as the AGV would travel, blue curve shows the resulting spline, and orange circles represent obstacles.

The navigation performance measurement experiment discussed previously in section II A. Vehicle Navigation can be similarly applied for obstacle detection and avoidance. In fact, the ASTM F45.02 subcommittee navigation and docking task groups have discussed the potentially overlapping nature of the two vehicle capabilities. The ASTM F45.03 Obstacle Detection and Protection subcommittee is currently in the process of considering standards in this area. Questions have been raised regarding standards development as follows:

1. How well does the AGV react to situations? For example:
   - Obstacles appearing in the path
   - Potential obstacles headed towards the path
   - Unstructured (i.e., changing obstacle locations) areas not on the original planned path or that rapidly change
2. How far off the commanded navigation path can an AGV be, and at what speeds, before it violates the path and causes a stop? For example, due to environmental factors such as:
   - Offset-pitched/rolled AGV can’t see guidance markers, such as reflectors, magnets, wire, etc.
   - Guidance or boundary-marking tape is worn or broken
   - Terrain causes “bouncing” or moving laser or other navigation sensors
3. How well does the vehicle react when a human is detected and how should the human be represented? For example:
   - By test pieces, mannequins, humans
   - With what coverings? (i.e., what clothes should be worn?)
4. How to interact with manual equipment (e.g., forklifts, machines)
5. How to standardize communication of vehicle intelligence for obstacle detection and avoidance? For example:
   - Contextual autonomy levels [4]
   - Situation awareness (e.g. LASSO) [14]:

Experiments to support ODA performance test method development will be performed based on forthcoming guidance from the ASTM F45 subcommittee. However, a prototype safety test method that has been developed to evaluate a vehicle’s response to obstacles in its path and within its stop zone, as noted in the Introduction, can be considered a first step towards full ODA standard test methods. ASTM F45 is meant to dovetail with safety standards such as ANSI/ITSDF B56.5. Therefore, providing an initial test method for detection of obstacles is ideal as a starting point for F45.03. The ‘Grid-Video’ detection method [3] provides a simple-to-implement test method that measures positional accuracy of the dynamic test piece relative to the vehicle position when the obstacle enters the vehicle path.

D. *6 DOF Optical Measurement of Dynamic Systems*

ASTM’s draft Standard for the Performance of Optical Tracking Systems that Measure Static and Dynamic Six Degrees of Freedom (6DOF) Pose (see Figure 10) is the next step beyond the static case covered by ASTM E2919-14 [8]. Optical tracking is being used for robot and autonomous vehicle GT measurement, as discussed in this paper. Optical tracking measurement systems [15] are used in a wide range of fields, including video gaming, filming, neuroscience, biomechanics, flight/medical/industrial training, simulation, and robotics. ASTM WK49831 is a working document that is considering both static and dynamic measurements of systems under test. The scope of the draft standard test method is to provide metrics and procedures to determine the performance of a rigid object tracking system in measuring the dynamic pose (position and orientation) of an object. Optical measurement systems may use the test method to establish the performance for their 6 DOF rigid body tracking pose measurement systems. The test method will also provide a uniform way to report the statistical errors and the pose measurement capability of the system, making it possible to compare the performance of different systems. So all the measurements can be traced to the standard.

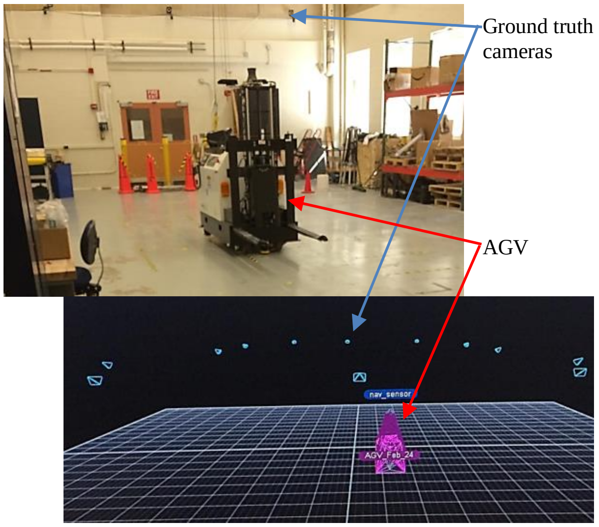


Figure 10. (top) autonomous vehicle test lab and (bottom) screenshot of the perception ground truth system space showing cameras and vehicle rigid body.

In the initial test procedure, measurements with uncertainties were computed using an artifact – namely a metrology bar as shown in Figure 9 (a). Current optical tracking systems utilize a three-marker metrology bar with all markers in a line which does not provide 6 DOF system performance measurement. A metrology bar made of carbon fiber with length 620 mm and with five reflective markers attached on each end was used as the 6 DOF artifact. A carbon fiber bar is used since it limits the effects of thermal expansion. The metrology bar markers on each end form a constant relative 6 DOF pose between the two ends. A shorter bar length should be used for smaller space measurements to maximize metrology bar movement during dynamic measurements.

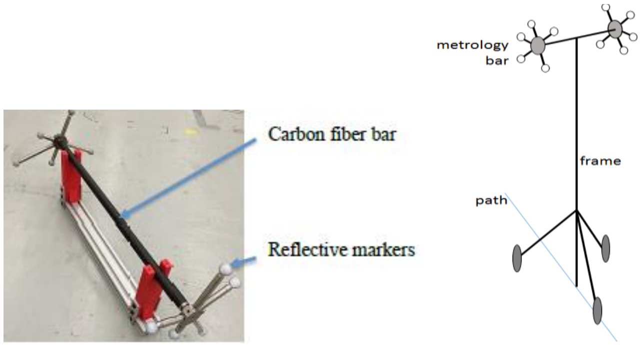


Figure 9. (a) Proposed metrology bar, (b) Example frame used to move the metrology bar.

Most optical tracking systems have at least a 30 Hz data collection rate. Therefore, a minimum of 5 min of data needs to be collected. The workspace is uniformly divided by the artifact length. The artifact is moved using at least the minimum and maximum motion capture velocity specified for the system.

The static test procedure for measuring the performance of the optical tracking system is to divide the test space into a grid and place the artifact at intersections of the grid and at various orientations. The dynamic test procedure also divides the test space into a grid where the metrology bar is moved in a raster scan pattern forward-to-back and left-to-right throughout the space.

The metrology bar maintains a constant separation and orientation of the two marker clusters along all the paths and can be rigidly attached to and moved using a wheeled frame as illustrated in Figure 9 (b) that is pushed/pulled by a human, a mobile robot, or other mover to closely follow the path.

The metrology bar is moved at the maximum specified velocity of the optical tracking. Pose error measurement and reporting methods are also described in the ASTM WK49831 [8] working document.

III. Conclusion

The AGV standards development process has been limited for many years to considering only safety standards. Starting in late 2014, ASTM F45 Driverless Automatic Guided Industrial Vehicles performance standards are being developed to include navigation, docking, terminology and several other key areas for AGV’s, mobile robots, and mobile manipulators. As discussed in this paper, standard test methods for measuring vehicle performance are being developed so that manufacturers and users of these systems can easily replicate the measurements in their own facilities and at minimal cost and effort. More AGV and mobile robot systems, instead of just the one AGV used in these experiments, would ideally validate the generic test method proposed.

A comparison of GT measurement systems was also made to support the test method development. It was determined that for dynamic AGV measurement, an optical tracking system provided a suitable ground truth measurement. At the same time, a standard for these dynamic measurement systems is also being developed. The standard will allow vehicle and robot performance standards developers to use the systems as ground truth with known measurement uncertainty. Optical tracking systems users and manufacturers can replicate the same test methods with similar tracking systems and use the results to compare their performance at dynamic tracking tasks.

ACKNOWLEDGMENT

The authors would like to thank the ASTM F45.02 subcommittee navigation task group and Omar Y. Aboul-Enein, Salisbury University student, for their recent input to navigation test method development and experimentation. Also, we thank Sebti Foufou, Qatar University, Doha, Qatar, for his guidance on the mobile manipulator docking performance measurement research.

REFERENCES

[1] ANSI/ITSDF B56.5:2012, Safety Standard for Driverless, Automatic Guided Industrial Vehicles and Automated Functions of Manned Industrial Vehicles, www.itsdf.org, Nov 2012.

[2] British Standard Safety of Industrial Trucks - Driverless Trucks and their Systems. Technical Report BS EN 1525, 1998.

[3] Bostelman, Roger, Will Shackleford, Geraldine Cheok, and Kamel Saidi. "Safe Control of Manufacturing Vehicle Research Towards Standard Test Methods." In Proc. International Material Handling Research Colloquium, pp. 25-28. 2012.

[4] Roger Bostelman, Elena Messina, “Towards Development of an Automatic Guided Vehicle Intelligence Level Performance Standard”, *Autonomous Industrial Vehicles: From the Laboratory to the Factory Floor*, Chap. 1, ASTM International, to be published 2015.

[5] Roger Bostelman, Tsai Hong, and Geraldine Cheok, “Navigation Performance Evaluation for Automatic Guided Vehicles”, IEEE International Conference on Technologies for Practical Robot Applications (TEPRA), Boston, MA, April 2015.

[6] ASTM International, Committee F45 on Driverless Automatic Guided Industrial Vehicles, www.astm.org/COMMITTEE/F45.htm, 2014.

[7] Roger Bostelman, Will Shackleford, "Obstacle Detection and Avoidance from an Industrial Automatic Guided Vehicle," IROS 2014.

[8] ASTM International, E57.02 Standard Test Method for Evaluating the Performance of Rigid Body Tracking Systems that Measure Dynamic, Six Degrees of Freedom (6DOF), Pose, Work Item #WK49831, June 2015.

[9] ASTM International E2919, Standard Test Method for Evaluating the Performance of Systems that Measure Static, Six Degrees of Freedom (6DOF) Pose, http://www.astm.org/Standards/ E2919-14.htm

[10] NDC 8 jAGV Control System, http://www.kollmorgen.com/en-us/products/vehicle-controls/electrical-vehicle-controls/ndc8/, 2015.

[11] Hvilshøj, Mads, and Simon Bøgh. "" Little Helper"-An Autonomous Industrial Mobile Manipulator Concept." International Journal of Advanced Robotic Systems 8, no. 2 (2011).

[12] Roger Bostelman, Tsai Hong, Jeremy Marvel, “Performance Measurement of Mobile Manipulators,” Proceedings SPIE DDS 2015, Baltimore, MD, April 2015.

[13] Burge, James H., Peng Su, Chunyu Zhao, and Tom Zobrist. "Use of a commercial laser tracker for optical alignment." In Optical Engineering+ Applications, pp. 66760E-66760E. International Society for Optics and Photonics, 2007.

[14] Drury, Jill L., Brenden Keyes, and Holly Yanco. "LASSOing HRI: analyzing situation awareness in map-centric and video-centric interfaces." In Human-Robot Interaction (HRI), 2nd ACM/IEEE International Conference, pp. 279-286. IEEE, 2007.

[15] “Motion Capture Software Developers in the US: Market Research Report,” IBISWorld 2014.

Mobile Manipulator Performance Measurement Towards Manufacturing Assembly Tasks

Roger Bostelman*[1,2], Sebti Foufou[3], Steve Legowik[4], Tsai Hong Hong[1]

*Corresponding author: roger.bostelman@nist.gov
[1]National Institute of Standards and Technology, Gaithersburg, MD 20899, USA
[2]Le2i, University of Burgundy, BP 47870, 21078 Dijon, France
[3]CSE Dept., College of Engineering, PO. Box 2713, Qatar University, Doha, Qatar
[4]Robotic Research, LLC, Gaithersburg, MD 20878, USA

Abstract. Mobile manipulator performance measurement research is relatively minimal as compared to that of robot arms. Measurement methods, such as optical tracking systems, are useful for measuring the performance of mobile manipulators, although at a much higher relative cost as compared to artifacts. The concept of using test artifacts demonstrates to potential manufacturers and users of mobile manipulator systems that relatively low cost performance measurement methods exist. This paper discusses the concept of reconfigurable mobile manipulator artifacts that were designed and built. An artifact was then used through experimentation to measure the performance of a mobile manipulator to demonstrate the feasibility of the test method. Experimental results show a promising test method to measure the performance of mobile manipulators that are to be used for manufacturing assembly tasks, where at least the mobile manipulator tested has the capability to perform assembly to 1 mm positional accuracy or greater.

Keywords: mobile manipulator, performance measurement, ASTM F45, artifacts, ground truth

1 Introduction

Mobile robots and mobile manipulators have been popular research topics [1, 2, 3, 4, 5]. But, in general mobile manipulators have been further investigated recently and are now becoming commercial tools for industrial use [6, 7, 8]. In research, considerations have focused on the coordination of movements of the robot and the base since redundant degrees-of-freedom (DoF) exist by adding the moving base. An example mobile manipulator consists of a six DoF robot arm (manipulator) mounted onboard a wheeled base (e.g., automatic guided vehicle (AGV) or mobile robot) with two translational and one rotational DoF in the horizontal plane for a total of nine DoF. [9]. Some mobile manipulators have more or fewer DoF and may also be equipped with vertical axis motion control of the robot arm base.

As with robot arm or AGV performance, it is important for manufacturers and users of mobile manipulators to implement performance measurements to understand their

Bostelman, Roger; Foufou, Sebti; Legowik, Steven; Hong, Tsai.
“Mobile Manipulator Performance Measurement Towards Manufacturing Assembly Tasks.”
Paper presented at the 13th IFIP International Conference on Product Lifecycle Management (PLM16), Columbia, SC, Jul 11-Jul 13, 2016.

system capabilities for appropriate application. For example, a user may wish to apply a mobile manipulator to assemble an engine having relatively high tolerances and associated costs as compared to inserting relatively low tolerance and cost rivets into sheet metal covers.

Measurements of the performances of mobile manipulators performing standard tasks (poses and motions) are non-existent except for simply ensuring that the task has been more or less completed. Robot performance measurements may include path comparison and path drawing, Cartesian and polar coordinate measuring, triangulation, optical tracking, inertial measuring, as well as the difference in position and orientation, or pose, of mainly the end of arm tooling from the commanded robot pose. Ground truth measurement using motion tracking systems of various techniques provides relatively accurate robot joint, segment, or tool point position information such that comparisons can be made to the commanded pose. Summarizing review of robot, mobile robot, and mobile manipulator performance measurement research shows this as being relatively new to the research community [10].

A survey of research on performance measurement of mobile manipulators [10] was published by the National Institute of Standards and Technology (NIST) as basis for research in the Robotic Systems for Smart Manufacturing (RSSM) Program [11]. The Program develops and deploys advances in measurement science that enhance U. S. innovation and industrial competitiveness by improving robotic system performance and other aspects to achieve dynamic production for assembly-centric manufacturing. Recently, NIST has been measuring performance of mobile manipulators using both a motion tracking system and artifacts designed at NIST. The artifacts can provide an inexpensive, yet low uncertainty method for manufacturers and users to measure the performance of mobile manipulators.

Performance standards, such as ASTM F45 [12], can also benefit from the use of low cost, high accuracy artifacts to develop generic test methods so that manufacturers and users perform similar and comparative tests. Specifically, ASTM F45.02 Docking and Navigation subcommittee is developing work item WK50379 [13] on docking unmanned ground vehicles and their onboard equipment, such as manipulators. In this work, the use of artifacts is being considered as ground truth for mobile manipulator performance measurement.

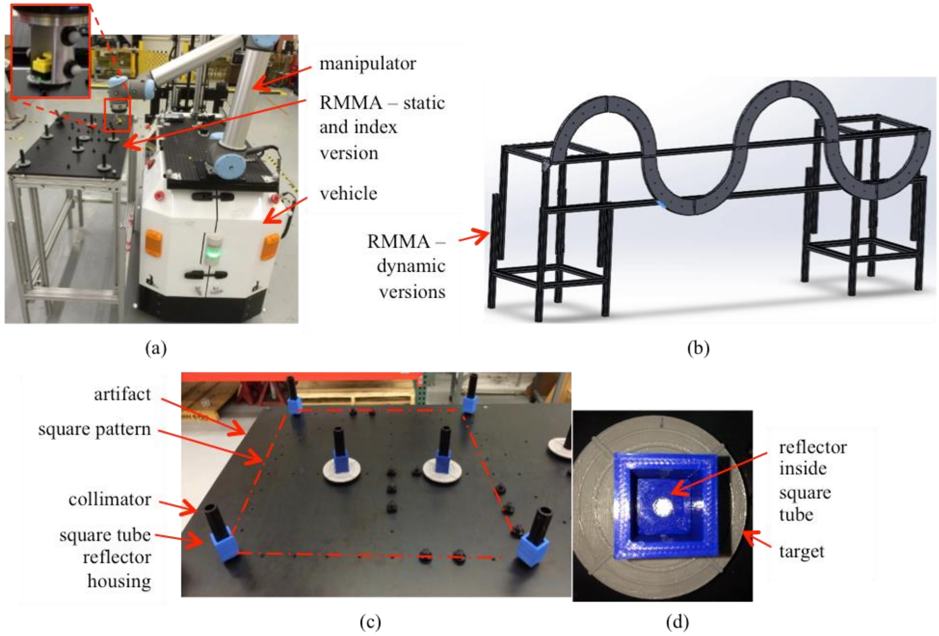
This paper discusses the design and use of the NIST artifacts, called reconfigurable mobile manipulator artifacts (RMMAs), in measuring mobile manipulator performance. The concept of using artifacts and programmed algorithms to control the manipulator are discussed. An experiment demonstrating feasibility and experimental results is then discussed followed by conclusions that suggest follow-on measurements.

2 Performance Measurement using Artifacts

The concept includes positioning a mobile manipulator next to an artifact as well as positioning and orienting the end of arm tool (EOAT) attached to the manipulator at specific locations above an artifact to digitally detect fiducials with known uncertainty. The performance evaluation criteria include the:

- Time to register the mobile manipulator to the artifact
- Time to move from the registration points to the assembly points
- Repeatability after registration
- Number of search steps equating to the initial distance from registration/assembly points
- Detection of reflectors with varying diameters

Artifacts, called reconfigurable mobile manipulator artifacts (RMMAs), were designed at NIST to include square, circle, triangle, straight and curved lines, and sinusoidal geometric patterns of tapped holes drilled into machined plates with tolerance of +/- 0.025 mm. The static and index artifact, RMMA-1, is shown in Figure 1(a) beside a mobile manipulator. A dynamic RMMA, RMMA-2, is shown in Figure 1(b). Static means a stopped vehicle with the only onboard manipulator moving to detect fiducials. Index means the mobile vehicle moves from one static location to another where the manipulator cannot physically reach all patterns from one stopped location. Dynamic means both a continuously moving vehicle and onboard manipulator to detect fiducials. Figure 1(c) shows a 457.2 mm square pattern of four reflector fiducials located at the square corners of RMMA-1 and Figure 1(d) shows a close-up of the reflector inside the square tube reflector housing (which also supports a collimator to be explained later).


manipulator
RMMA – static and index version
vehicle
RMMA – dynamic versions
artifact
square pattern
collimator
square tube reflector housing
reflector inside square tube
target

(a) (b)

(c) (d)

Figure 1: Reconfigurable mobile manipulator artifacts (RMMAs) showing (a) static and index version (RMMA-1) and (b) dynamic version (RMMA-2). (c) Static and index version square pattern of reflectors and (d) close-up, top view of an illuminated reflector inside the square tube. The inset in (a) shows the retroreflective laser sensor used to detect reflectors.

Both RMMAs can be in a horizontal (as tested in this research), vertical, or other orientation, at short-to-tall heights, and even configured overhead as would be typical of assembly in manufacturing facilities for an unlimited set of performance measurement possibilities. The EOAT was a retroreflective laser sensor (RLS) that emits light to a reflector and is detected by the RLS. A camera, with a light source, could instead be used as the detection sensor, especially with a larger diameter reflector or other spot. For the RLS/reflector concept, no camera software algorithm was required as the RLS connected directly into one of the manipulator digital inputs. The reflectors can have specific diameters depending upon the required uncertainty for their location. The manipulator[1] used has manufacturer's specified repeatability of 0.1 mm [14] and the AGV navigation sensor has manufacturer's specified resolution of 1 mm [15]. No information is provided by the AGV manufacturers to specify the vehicle performance such as position accuracy. As published in [16], 6.3 mm diameter reflectors were used to test mobile manipulator uncertainty as an initial concept feasibility test.

For our tests, detector-to-reflector distance parallel to the laser axis was approximately 127 mm where the minimum and maximum detection distances are 100 mm and 10 m respectively. The distance would be representative of a programmed waypoint above and in-line with the next manipulator task point aligned to grip or insert a part or perform another task. The desired uncertainty may be, for example, a part insertion alignment tolerance required for a manufacturing assembly process. Moving along this grip/insertion line, parallel to the laser, at the aligned pose to the task point, also provides some knowledge of insertion performance (i.e., if the task point is continuously detected along the grip/insertion line).

Each adapter, to be screwed into the various patterns of holes, supports a background target, a circular reflector, a square tube reflector housing, and a cylinder used as a light collimator. Circular collimators are inserted into three dimensional (3D) printed (blue) square tubes that house a micro reflector, a reflector cover with a specific diameter hole, through which exposes the reflector, on top of the reflector and the collimator on top of the cover. Flat background targets, measuring 7.6 cm diameter with 6.4 mm incremental rings are perpendicular to each collimator and sometimes used as a simple visual cue for the test director when the manipulator does not align with the reflector. The adapter, reflector, housing, target, and collimator can be perpendicular to the flat surface or rotated to pitch angles between ± 90° and yaw angles between 0° and 360°. The reflector and the collimator inside can be any diameter, dependent upon the sensor specification and the desired measurement uncertainty. Experiments for this paper utilized 1 mm through 6.3 mm diameter reflector cover holes where the 1 mm diameter hole was used for registering the manipulator to the reflector center.

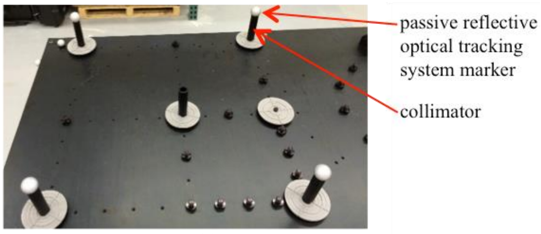
Without the collimator, as shown in Figure 1(c), the reflector can be detected at approximately ± 20° to the vertical axis. For the collimators used, the reflector can be detected at a maximum 3.2 mm radius from the reflector center. It can be detected at

[1] Disclaimer: Commercial equipment and materials are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

approximately ± 7° to the vertical axis when using a 12.7 mm inside-diameter collimator. Collimators could be made with even smaller inside-diameters to force more perpendicular manipulator tool point axis pose to the reflector.

The RLS, shown in Figure 1(a), shows the sensor mounted in-line and perpendicular to the manipulator tool point. Initial alignment to the reflector can occur using one of several methods briefed in [16]. For our experiments, we aligned the RLS using the manipulator jog mode from the teach pendant until the laser detected the two registration reflectors for both the circle and square reflector patterns. Therefore, we could read directly from the teach pendant the end-effector coordinates to return to during our experiment.

An optical tracking measurement system was initially used as ground truth [17] for comparison to the use of artifacts and to measure all system components simultaneously for test method development. The ground truth system has static positional accuracy of 0.02 mm, however costs approximately 20 times the cost of the artifact concept. Figure 2 shows a snapshot of the optical tracking system markers used as fiducials and positioned on the square pattern of collimators. The tracking system measured the performance of the vehicle, manipulator, and artifact within the same system of reference. In this paper, the focus is to discuss the comparison between only the manipulator and artifact as a low cost, relatively high accuracy measurement method. The potential for artifacts being made using three dimensional (3D) printing could lower the cost further by an order of magnitude, or 200 times, as demonstrated through machining costs of the RMMAs and the 3D printing of parts used with the artifact.



(a)

Figure 2: RMMA with optical tracking system markers on each collimator. Markers are also shown in Figure 1(a) attached to the retroreflective laser sensor held by the manipulator.

3 Experiments

The experiment consisted of moving the AGV from a home position away from the RMMA-1. The AGV control program moved the AGV to the first location where its position and orientation or pose was pre-determined by the AGV control program. AGV orientation angles were programmed to be at 45° with respect to the RMMA-1. Upon completion of the pattern detection for a location, the AGV moved to the second location and pose, and so forth until six locations were completed. The AGV completed the test by returning to the home position.

A modified registration method for registering the mobile manipulator to the RMMA was recently developed that uses the components shown in Figure 3, including a 3D printed aperture housing, collimator, micro-reflector, and a camera iris aperture. The aperture allows the opening to the reflector to not only be any size, but to also center the opening. This ensures that the two registration fiducials are centered on the reflector even when using a much larger reflector for all other fiducials. The smallest aperture opening used was 1 mm diameter while all other fiducials were 3.2 mm or 6.3 mm diameter. The RLS did not return a ‘detect’ at a smaller diameter than 1 mm diameter aperture setting.

A circular search pattern was used in previous tests [16] to register the manipulator to the first reflector. Once the first fiducial was acquired, it was possible for a registration skew to occur as only the edge of the pattern may have been detected and the opposite side of the second fiducial used for registration could cause an incorrect performance measurement of the mobile manipulator. The circular search began with a step increment chosen to be approximately half of the diameter of the fiducial being tested. For example, an initial step size of 3.1 mm was chosen for a 6.3 mm fiducial to be detected. However, after the initial circle of steps was completed, the step moved to the next larger 3.1 mm circle step radius (e.g., from 3.1 mm to 6.2 mm radius from the start location) and at the same step arc angle (e.g., 15°) causing much larger steps to occur as the circle pattern grew. Instead, a square pattern was tested for the research described in this paper that kept the same step size throughout the entire search. An example of the square step pattern is shown in Figure 4 where the search begins away from the reflector at the chosen start point (yellow arrow dotted end) and each step moves along the small white or gray arrows until the RLS detects the reflector with the red arrow step.

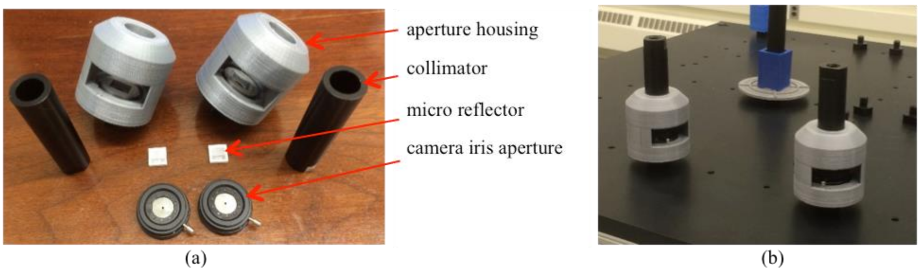


Figure 3: (a) Components used for registration and (b) registration fiducial mechanism attached to the RMMA.

The Mobile Manipulator program controlled the manipulator during the tests. It interfaced with the AGV directly to obtain the current AGV position and orientation, and it interfaced with the AGV control program (Transport Structure) running on the Order Manager application to coordinate the motion of the arm with the motion of the AGV. The AGV control program signaled the Mobile Manipulator program when it arrived at one of the stop or test locations. The AGV control program also sent the identification number of the test location. The Mobile Manipulator program read the current AGV pose and used it to compute the initial search location of the two registration reflectors in the target pattern (circle or square). Additional patterns could also have been used in the Mobile Manipulator program.

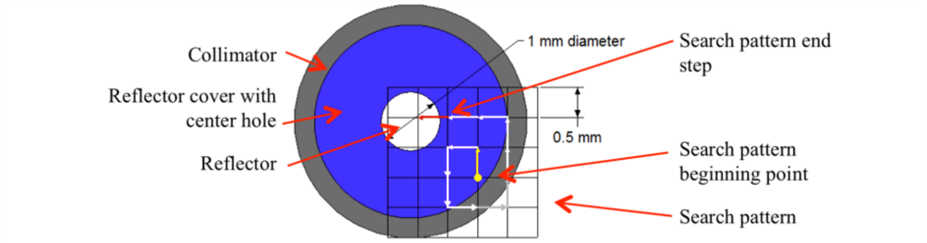


Figure 4: Example square step search pattern drawing. The pattern begins with the yellow arrow dotted end and ends when the reflector is detected with the red arrow search step.

The manipulator was first moved from a stowed location over the body of the AGV to a staging location directly in front of the AGV. The manipulator was then moved from the staging location to the first of the two registration reflectors. The staging location was chosen so that the manipulator could make a straight line motion from the staging location to a registration reflector located in front of, or to either side of, the AGV without colliding with its shoulder joint. After moving to the first registration reflector, the manipulator performed a square spiral search to determine the exact location of the reflector. When it determined the location of the first registration reflector, the program repeated the process with the second registration reflector. When the locations of the two registration reflectors were determined, the program had sufficient information to compute the locations of the other fiducials in the square or circular patterns. The initial search was not counted as a performance criteria since the mobile manipulator could use various types of registration techniques, such as: physical contact using a touch probe [18], cameras detecting fiducials [19], or laser interferometry, theodolites, and coordinate measuring arms [20]. However, for comparison to repeatability, the initial registration number of iterations count was logged and included in results.

Once the locations of all reflectors in the pattern were computed, the manipulator cycled through them a set number of times – 32 times for each pattern in this experiment. At each reflector, the RLS checked to see if the manipulator was aligned with the reflector.

When the test was completed, the manipulator was moved to the staging location and then the stow location. When the manipulator was back in the stow location, the Mobile Manipulator program signaled to the AGV control program that it was clear to move.

The positions of the index fiducials for the targets were recorded prior to performing the repeatability tests. The AGV was first moved to a location where it could reach both of the index fiducials. The current location and orientation of the AGV was recorded. The arm was repositioned manually until the sensor detected alignment with each of the index fiducials, and the manipulator position was recorded. This information, along with the manipulator base position relative to the vehicle's coordinate system, allowed the correct manipulator coordinates for the index fiducials to be calculated for an arbitrary AGV location. This allowed the AGV to approach the target/work area from any direction and to compensate for variation in the AGV's stopping pose.

The calibration of the manipulator base location involved recording the position of one or more fiducials from a variety of locations. Both the AGV location and the manipulator coordinates of the fiducials were recorded. This data was processed using an iterative, non-linear model to find the best value of the base position and orientation.

4 Results

The mobile manipulator performance measurement results using the RMMA-1 included only the detection of reflectors for each pattern and after initial registration. By comparison, the initial number of search steps used to register the manipulator at the first reflector was recorded. Results are shown in Table 1. The repeatability performance measurement process began once the mobile manipulator was registered to the artifact after initial registration and moving through the square or circle pattern one time and with the AGV statically positioned at a pattern. Measurements of 'detect' or '1' were logged for each RMMA-1 reflector location. If a search was required to find the fiducial after registration, the measurement at that reflector was counted as a 'no detect' and the number of search steps was recorded.

Table 1 shows: the consecutive position number and programmed AGV position, the AGV pose angle (heading), the circle or square pattern being detected, the total number of reflectors to detect for 32 pattern iterations after the registration pattern, the reflector diameters for each pattern (rounded to whole numbers), the number of reflectors detected and detection percentage, and the initial number of search steps needed to register to the first reflector after the AGV stopped. The AGV stop points programmed are shown in Figure 4. The lines leading to the stop points indicate the AGV orientation.

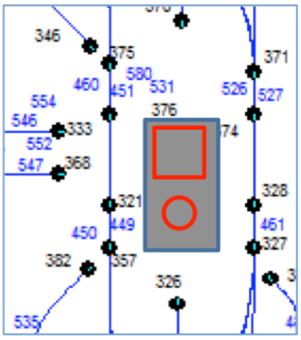
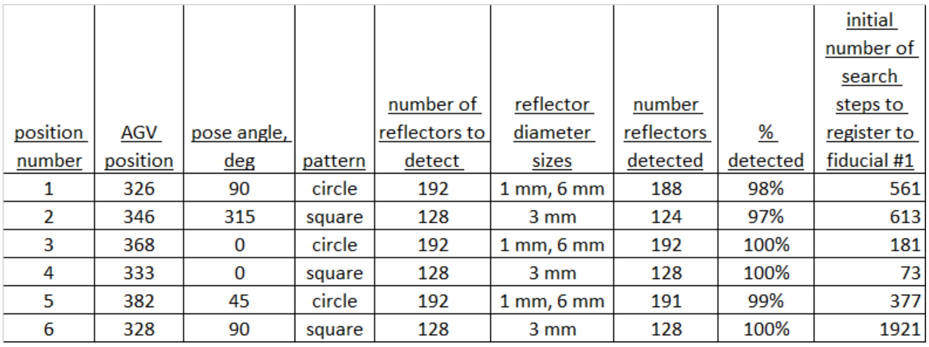


Figure 2: Stop points

The table shows very high repeatability results at 97% or above as shown in the "% detected" column of the table. The results demonstrate a good test procedure for determining repeatability of a mobile manipulator to register to and access assembly points within the reflector diameters chosen. Further tests are required to understand direct connections between mobile manipulator performance and system pose, for example, suggesting that AGV pose at 0° provides higher performance than at other angles. Results here do not show this since position 6 included the AGV being at 90° and yet, was repeatable to 100%. Several additional tests are envisioned as well, such as: repeatability of the same pattern followed by the other pattern, both from different AGV poses; using the 1 mm registration reflectors for all patterns followed by the same size reflectors for all, such as 3 mm; and using 1 mm diameter reflectors for all points within each pattern to provide a possible detection limit.



position number	AGV position	pose angle, deg	pattern	number of reflectors to detect	reflector diameter sizes	number reflectors detected	% detected	initial number of search steps to register to fiducial #1
1	326	90	circle	192	1 mm, 6 mm	188	98%	561
2	346	315	square	128	3 mm	124	97%	613
3	368	0	circle	192	1 mm, 6 mm	192	100%	181
4	333	0	square	128	3 mm	128	100%	73
5	382	45	circle	192	1 mm, 6 mm	191	99%	377
6	328	90	square	128	3 mm	128	100%	1921

Table 1: Test results of the mobile manipulator accessing the RMMA from various Stop Points (see Figure 4) and various AGV poses. The gray rectangle in the center of the Stop Points map shows the approximate RMMA square and circle pattern locations.

5 Conclusion and Future Work

As discovered in a NIST survey of mobile manipulator research [10], performance measurement of these systems is minimal as compared to robot arms. Measurement methods, such as using optical tracking systems, are useful methods for measuring mobile manipulator performance, although at a much higher cost. The use of known artifacts, called reconfigurable mobile manipulator artifacts, to measure the performance of mobile manipulators is being researched at NIST to demonstrate the feasibility of the test method. The concept of using artifacts demonstrates to potential manufacturers and users of mobile manipulator systems that relatively low cost performance measurement methods exist. Artifacts, such as the RMMA-1 and in the future, RMMA-2, allow an unlimited number of performance measurement configurations. The measurement of mobile manipulator repeatability and accuracy for very low resolution tasks (e.g., positioning bags of product) through very high resolution tasks (e.g., assembly of parts for manufacturing) is achievable through the use of RMMAs. Static and index tests have been completed using this method and have proven feasible. Experimental results show a promising test method to measure performance of mobile manipulators that are to be used for manufacturing assembly tasks, where at least the mobile manipulator tested has the capability to perform assembly to 1 mm positional accuracy or greater. Future test method developments should not only include dynamic mobile manipulator performance measurements, but also include the suggested tests in the results section. Additionally, rapid registration techniques, finer retroreflective laser sensors allowing smaller diameters, and in turn, physically providing peg-in-hole measurements with variable peg and hole chamfers, are expected to provide even higher performance measurements towards assembly applications of mobile manipulators.

References

[1] M. Shneier and R. Bostelman, “Literature Review of Mobile Robots for Manufacturing,” NIST Internal Report #8022, 2014.

[2] D. Katz, E. Horrell, Y. Yang, B. Burns, T. Buckley, A. Grishkan, V. Zhylkovskyy, O. Brock, and E. Learned-Miller, “The UMass mobile manipulator UMan: An experimental platform for autonomous mobile manipulation.” Workshop on Manipulation in Human Environments, at Robotics: Science and Systems, 2006.

[3] B. Hamner, S. Koterba, J. Shi, R. Simmons, and S. Singh, “An autonomous mobile manipulator for assembly tasks,” Autonomous Robot (2010) 28: 131–149. DOI 10.1007/s10514-009-9142-y

[4] S. Djebrani, A. Benali, and F. Abdessemed, “Modeling and Control of an Omnidirectional Mobile Manipulator,” Int. J. Appl. Math. Comput. Sci., 2012, Vol. 22, No. 3, 601–616 DOI: 10.2478/v10006-012-0046-1

[5] J. Vannoy and J. Xiao, “Real-time Adaptive Motion Planning (RAMP) of mobile manipulators in dynamic environments with unforeseen changes,” in IEEE Trans. on Robotics, 1199—1212, 2008.

[6] “Yaskawa Motoman MH80 robot unloading trucks - from Wynright Corporation,” http://www.youtube.com/watch?v=8wngL0BnF_4, June 18, 2013.

[7] E. Guizzo, “Meka Robotics, Announces Mobile Manipulator With Kinect and ROS,” http://spectrum.ieee.org/automaton/robotics/humanoids/meka-robotics-announces-mobile-manipulator-with-kinect-and-ros, 16 Feb 2011.

[8] T. Green, “KUKA Falls First, Buys Swisslog for $335M. Who’s Next?,” Robotics Business Review, Sept 29, 2014.

[9] W. Miksch, D. Schroeder, “Performance-Functional Based Controller Design for a Mobile Manipulator,” . Proceedings IEEE International Conference on Robotics and Automation, 12-14 May 1992.

[10] Roger Bostelman, Tsai Hong, Jeremy Marvel, “Survey of Research for Performance Measurement of Mobile Manipulators”, to be published in Journal of National Institute of Standards and Technology, 2016.

[11] Robotic Systems for Smart Manufacturing Program, http://www.nist.gov/el /isd/ms/rssm.cfm, National Institute of Standards and Technology, 2016.

[12] ASTM F45 Committee on Driverless Automatic Industrial Vehicles, www.astm.org, 2016.

[13] ASTM F45.02 Docking and Navigation subcommittee, work item WK50379, www.astm.org, 2016.

[14] Universal Robots A/S-UR10 User Manual, Version 3.0 (rev. 15167), 2014.

[15] SICK 2D Laser Scanners, https://www.sick.com/media/pdf/1/41/841/ dataSheet_LMS100-10000_1041113_en.pdf.

[16] Roger Bostelman, Tsai Hong, Jeremy Marvel, “Performance Measurement of Mobile Manipulators”, SPIE 2015, Baltimore, MD, April 2015.

[17] Roger Bostelman, Joe Falco, Mili Shah, and Tsai Hong Hong, “Dynamic Metrology Performance Measurement of a Six Degree-Of-Freedom Tracking System used in Smart Manufacturing”, ASTM International “Autonomous Industrial Vehicles: From the Laboratory to the Factory Floor” book chapter, 2016.

[18] MasterCal, http://www.americanrobot.com/products_mastercal.html, 2005.

[19] C B. Atcheson, F. Heide, and W. Heidrich, “CALTag: High Precision Fiducial Markers for Camera Calibration,” Vision, Modeling, and Visualization, 2010.

[20] Jose Mauricio, S. T. Motta, “Robot Calibration: Modeling Measurement and Applications,” Industrial Robotics: Programming, Simulation and Applications, Low Kin Huat (Ed.), ISBN: 3-86611-286-6, InTech, 2006.

Mobile Robot and Mobile Manipulator Research Towards ASTM Standards Development

Roger Bostelman[123], Tsai Hong[2]
[2]National Institute of Standards and Technology, Engineering Laboratory, Intelligent Systems Division, 100 Bureau Drive, MS8230, Gaithersburg, MD 20899
[3]IEM, Le2i, Université de Bourgogne, BP 47870, 21078 Dijon, France

Steven Legowik
Robotic Research, LLC
Gaithersburg, MD 20878

Abstract

Performance standards for industrial mobile robots and mobile manipulators (robot arms onboard mobile robots) have only recently begun development. Low cost and standardized measurement techniques are needed to characterize system performance, compare different systems, and to determine if recalibration is required. This paper discusses work at the National Institute of Standards and Technology (NIST) and within the ASTM Committee F45 on Driverless Automatic Guided Industrial Vehicles. This includes standards for both terminology, F45.91, and for navigation performance test methods, F45.02. The paper defines terms that are being considered. Additionally, the paper describes navigation test methods that are near ballot and docking test methods being designed for consideration within F45.02. This includes the use of low cost artifacts that can provide alternatives to using relatively expensive measurement systems.

Keywords: mobile manipulator, reproducible performance, smart manufacturing, ground truth, test methods, artifact

1 INTRODUCTION

United States [1] and European [2] safety standards for industrial vehicles have evolved to protect people working near automatic guided vehicles (AGVs). However, performance standards for AGVs[2] and mobile robots have only recently begun development. Similarly, safety and performance of these industrial vehicles with onboard equipment, such as robot arms, are beginning to evolve.

The National Institute of Standards and Technology (NIST), Robotic Systems for Smart Manufacturing (RSSM) Program [3] is currently researching both AGV and mobile manipulator performance. The Program develops and deploys advances in measurement science that enhance U. S. innovation and industrial competitiveness by improving robotic system performance and other aspects to achieve dynamic production for assembly-centric manufacturing. NIST has recently been measuring performance of AGV navigation towards development of test methods that can allow vehicle manufacturers and users to match their systems to tasks such as for safe, material handling. Additionally, advanced mobile manipulators are being sold as useful tools for unloading trucks [4] and for delivering, placing, and manipulating semiconductor waferpods within wafer fabrication facilities [5]. In these two cases, both AGVs and mobile robots support onboard manipulators to provide smart navigation and docking capabilities.

[1] roger.bostelman@nist.gov; phone 1-301-975-3426; fax 1-301-990-9688

[2] Disclaimer: NIST does not endorse products discussed within this paper nor manufacturers of these products. Products mentioned are for information purposes only and are not expressed as an endorsement for them or their manufacturer.

In 2014, ASTM Committee F45 for Driverless Automatic Guided Industrial Vehicles [6] was established to develop standardized nomenclature and definitions of terms in this area. ASTM F45 is developing a terminology working document [7]. Some terminology will be briefly discussed in this paper.

ASTM F45 also recommends practices, guides, test methods, specifications, and performance standards for driverless automatic guided industrial vehicles. The Committee encourages research in this area to facilitate the development of such standards. In support of ASTM F45, NIST is currently developing test methods for navigation and docking. Navigation test methods for “defined” areas, such as within barriers or along pedestrian paths, are being developed by the Task Group within ASTM F45.02 Docking and Navigation. These methods are described in a working document [8] and they are being reduced to practice at NIST. Additionally, performance test methods for vehicle docking and vehicle-with-onboard-equipment (e.g., mobile manipulator) docking are being developed at NIST and proposed to F45.02. The experiments and results that support the test methods are described in section 4. Conclusions end the paper and provide next steps for ASTM F45 standards development.

2 ASTM F45.91 TERMINOLOGY

The term ‘AGV’ has been used throughout industry and research since the 1950’s [9]. ‘Mobile robot’ has been used throughout the research community for perhaps the same length of time and the term ‘unmanned ground vehicle (UGV)’ has been used in the military and industrial security organizations. A single term is ideal to limit confusion by vehicle users and so that various performance test methods developed can be considered for any vehicle type, potentially independent of autonomy level and vehicle capability.

The ASTM F45.91 Terminology [7] task group is developing a working document to address this disparity of terms. As stated in the F45.91 scope: “For the terminology to be harmonious with the practices in the field, definitions have been drawn from the literature or other public sources when possible. When no definition is available, or definitions are in dispute, a consensus-based approach will be employed to resolve definitions”. For example, the task group decided on a core term, ‘UGV’, that provides levels of autonomy instead of several different terms being used to define the variety of industrial vehicles. The proposed UGV term, associated sub-terms, and definitions are as follows:

- Unmanned Ground Vehicle (UGV), noun -vehicle that operates while in contact with the ground without a human operator (see: Automatic – UGV, Automated – UGV, Autonomous – UGV)
    - automatic - UGV, noun -vehicle capable of following a pre-programmed path and that does not deviate from the path without human intervention; see A-Unmanned Ground Vehicle.
    - automated - UGV, noun -automatic vehicle with limited ability to deviate from the pre-programmed path; see A-Unmanned Ground Vehicle.
    - autonomous - UGV, noun -self-guided vehicle that is able to travel without a pre-programmed path and operates independently to navigate around fixed and moving obstructions; see A-Unmanned Ground Vehicle.

The concept allows for the ‘automatic guided vehicles’ term to keep the sub-term ‘automatic’ in Automatic – UGV, while mobile robots with typically increased autonomy and capabilities may be considered as Autonomous – UGVs. A vehicle with more capability and autonomy than an Automatic – UGV, yet less than an Autonomous – UGV would be considered an Automated – UGV. However, all three terms have a single, base ‘A-UGV’ term that will be used throughout ASTM F45 subcommittee test methods as they are developed. The generic test methods can therefore, focus on a single test to be performed by all types of A-UGVs where applicable.

Terms within the F45.91 working document are based on three sources: American National Standards Institute/Industrial Truck Standards Development Foundation (ANSI/ITSDF) B56.5 [1], International Standards Organization (ISO) 8373 [10], and the Material Handling Industry of America [11] list of terms. The term ‘robot’ was removed from the original draft working document during pre-ballot comment resolution to limit confusion, since ‘manipulator’ was expected to be used more frequently, and to minimize confusion of an onboard A-UGV robot arm.

3 ASTM F45.02 DOCKING AND NAVIGATION

As briefed in the Introduction section 1, NIST is developing navigation and docking performance test methods as part of the RSSM Program and in support of ASTM F45. Specifically, navigation test methods for defined areas and both vehicle docking and vehicle-with-onboard-equipment (e.g., mobile manipulator) docking are being developed at NIST. The standard does not address safety concerns. These are covered in B56.5 [1]. The following sub-sections detail the navigation and docking test methods.

3.1 Navigation

As stated in the ASTM F45.02 Navigation: Defined Areas working document, statistically significant test results are to demonstrate that the A-UGVs traverse paths that are typical in manufacturing facilities and warehouses having defined and undefined areas that are structured and unstructured. A single performance test method is expected to evaluate whether or not an A-UGV deviates from its intended path. Additionally, the same test method will also allow vehicles to use local environment features as input for navigation as needed.

The scope in the current F45.02 Navigation working document includes the proposed test method to evaluate an A-UGV "capability of traversing through a defined space (e.g., navigation areas with limited A-UGV clearance)". It is expected that A-UGV manufacturers, installers, and users will use F45.02 to evaluate industrial vehicles that navigate between structures defining the vehicle path with typical constraints such as walls, equipment, and pedestrian paths and other user application requirements.

The F45.02 navigation performance test method consists of traversing scalable areas defined by physical barriers, virtual barriers, and/or floor markings. The defined navigation test is a straight corridor followed by a 90 degree turn into a second corridor. The corridors are constructed with a width sufficient for the A-UGV to traverse them. The path width is incrementally reduced during A-UGV evaluation. The corridor is reduced and the A-UGV is tested, "until the most constrained testing pathway is accomplished for the specified number of repetitions". The A-UGV configuration of software, hardware, and other characteristics are to remain the same during the entire test. During the test, the A-UGV traverses the path from the start point to the end point, and then returns back to the start point. For the return trip, the A-UGV can either drive backwards, or turn around. The full start-to-goal-to-start traversal of the test course is considered one full repetition.

Figure 1 shows three test method configurations proposed in F45.02 and evaluated at NIST. The three configurations include physical barriers, virtual barriers (e.g., laser beams), and floor markings. Physical barriers, shown in Figure 1a, are temporary walls used for the experiments were made of painted, 1.2 m square oriented strand board mounted to 0.6 m bases. The barriers were aligned to form a corridor approximately with a length of four vehicle lengths, 8 m, and a variable width. The initial width is chosen to provide a certain buffer from the A-UGV sides defined by the safety sensor side distance plus a chosen uncertainty (standard deviation) distance (e.g., 10 cm). After each test, if no wall detection occurs during traversal, the walls are moved towards the A-UGV sides by a chosen amount, e.g., 2 cm. When the wall is detected during a test, the detection is logged in a report and the test is repeated. A statistically significant number of trials (a minimum of 30) are done by the A-UGV provider dependent upon the confidence and probability of success threshold (PST) desired (e.g., 0.95 confidence with 0.95 PST = 118 trials). Additional details of the barrier test setup are provided in [12].

Figure 1b shows the virtual barrier test setup which makes use of a laser breakbeam aligned along the vehicle path. The test setup and procedure are similar to the physical barrier setup where the laser line is initially set and moved using a procedure similar to that of the physical barriers. However, to break the laser beam, as opposed to detecting a physical barrier, a bar measuring the desired width is clamped perpendicular to the vehicle. The bar protrudes from the vehicle at the laser breakbeam height. The distance the bar projects is determined by the lane width plus the chosen uncertainty (e.g., 2 cm). Similar trial repetitions are then completed as with the physical barriers.

Figure 1c shows the floor marking test setup that includes a bar similar to that used in the virtual barrier test setup. This supports a laser pointer or marking pen pointed at or touching the floor, respectively. The test setup and procedure are similar to the virtual barrier setup where the laser line is initially set and moved using a similar procedure to that of the physical barriers. A line is attached to the floor (e.g., pedestrian marker, painted or taped line) at the location of a virtual barrier laser breakbeam. Additionally, the laser pointer/marker is incrementally moved closer to the A-UGV along the bar for each successful trial. Again, similar trial repetitions are then completed as with the physical and virtual barrier test setups.

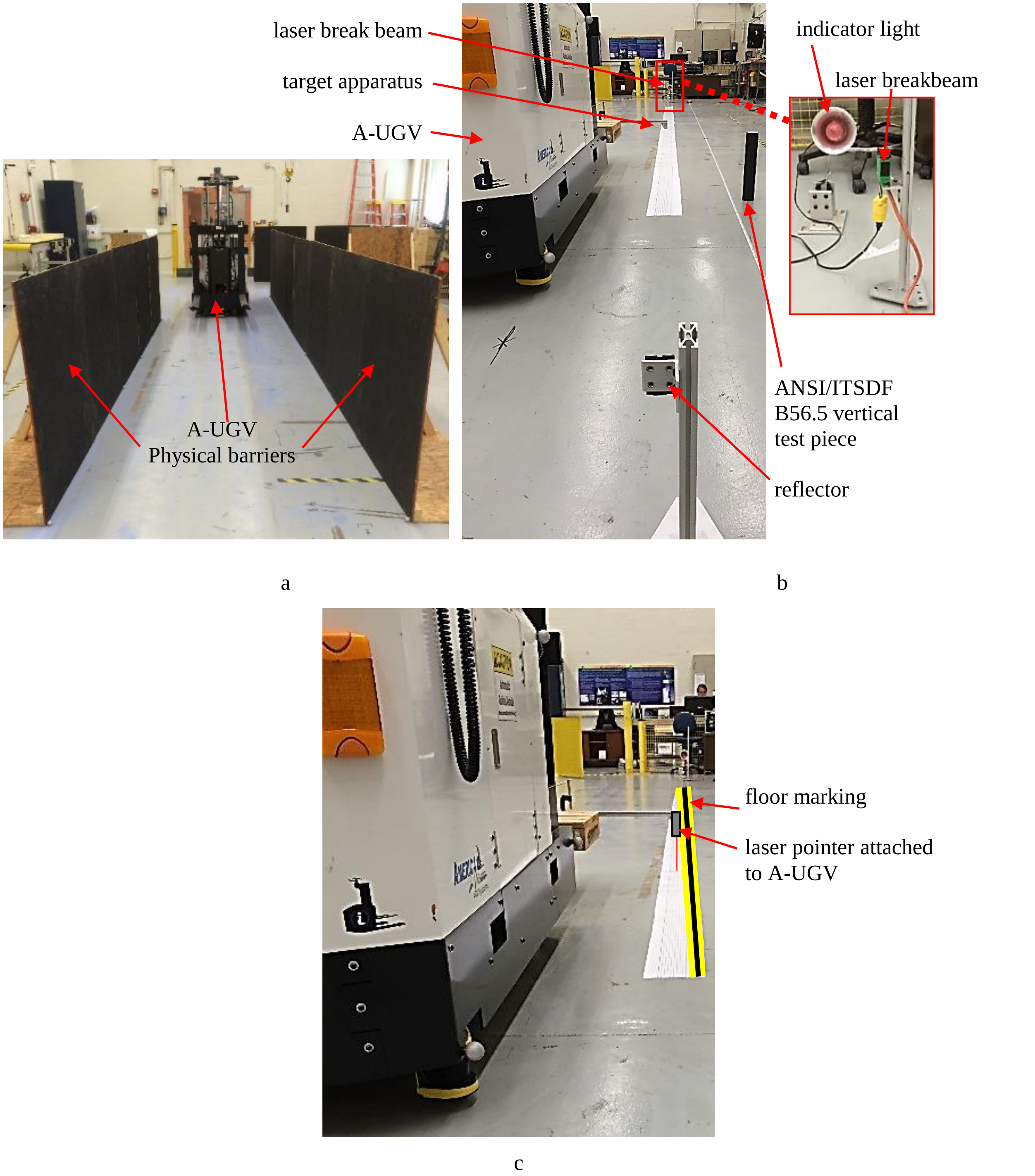


Figure 1. Example A-UGV navigating within a) physical barriers, b) virtual barriers (e.g., laser beams), and c) floor markings.

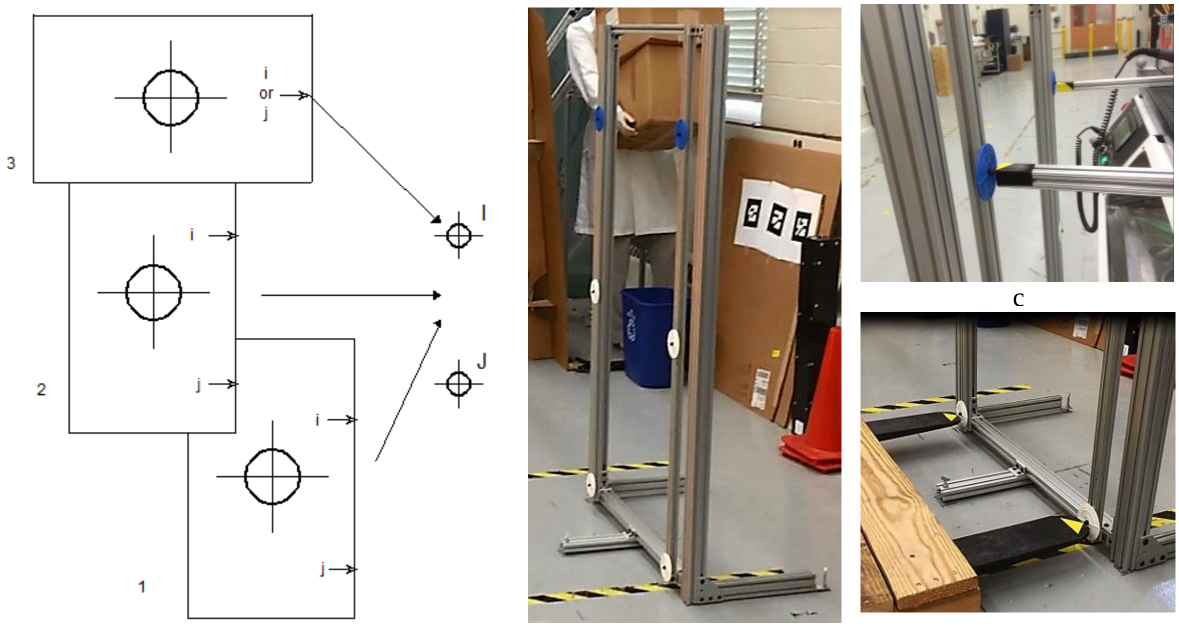
3.2 Docking

3.2.1 Vehicle Docking

A-UGVs "dock" with different devices in their work area. Vehicles with forks typically dock with pallets. Unit load vehicles dock with tray stations. Tugger style vehicles dock with hitches. These vehicles have different but related positioning requirements for docking. Fork-style vehicles must align their forks perpendicular to the openings of a pallet. Unit load vehicles must align properly with a tray station in order to allow a tray to roll between the onboard-vehicle roller table and a facility roller table. The vehicle roller table has right and left edges that align with the corresponding edges of the facility tray station. Docking for these two types of vehicles can be generalized into the act of aligning two points on the vehicle with two points on the device. Similarly, tugger vehicle docking can be generalized as aligning one point on the vehicle with one point on the device (representing the hitch).

A-UGV users might assume that their vehicles remain calibrated from vehicle installation, although these vehicles can become uncalibrated. An experiment using a two year old, uncalibrated A-UGV that was programmed to stop at various points yielded an uncertainty range of approximately 1 mm to 50 mm [12] as measured by a laser tracker. Docking was measured again after the A-UGV was calibrated using the manufacturer's procedures. During tests, the A-UGV approached similar dock locations and after A-UGV calibration, provided consistent 5 mm uncertainty (standard deviation) from several dock points in the lab.

NIST and the F45.02 subcommittee have begun investigating A-UGV docking performance test methods. The generic concepts of vehicle docking, aligning one or two points, was tested at NIST [12] and proposed to the ASTM F45.02 subcommittee. Figure 2(a) illustrates the candidate tests. Three vehicles are shown, represented as rectangles. Vehicles 1 and 2 each have two points, i and j, that must align with the two points on the device, I and J. Vehicle 3 has only one point that must be aligned with one point on the device, either I or J.



a b c d

Figure 2. Docking Test Method. (a) Conceptual docking test method for use with various A-UGVs. The three rectangles represent three different vehicles, each with one or two points, i and j, that must be aligned with one or two target points on the device, I and J. (b) Docking apparatus with multiple alignment target points, lower and middle white targets and upper blue targets. (c) Unit-load A-UGV docked with the Docking apparatus. Two bars

represent roller table edges that should align with the two blue targets. (d) Fork-type A-UGV docked with the Docking apparatus. The forks should align with the two white targets.

Figure 2(b) shows the NIST Docking apparatus. It has leveling feet and targets moveable in both lateral and vertical directions used to test one- and two-point docking with the targets. Targets have a center point with 3 mm spaced concentric rings to visually detect relative alignment uncertainty. The targets can be sized for other specific desired relative alignment uncertainty.

3.2.2 Vehicle with Onboard Equipment Docking

Vehicles with onboard equipment, such as robot arms (manipulators), are typically called mobile manipulators. NIST has also been developing performance test methods for mobile manipulators that will be affordable by manufacturers and users. These test methods are also useful to ASTM F45.02 as docking test method reference experiments of vehicles with onboard equipment. The method is feasible for measuring performance of mobile manipulators. The mobile manipulator positions a relatively inexpensive laser retroreflective laser to detect smaller and smaller reflective targets accurately positioned on an artifact.

NIST developed a test apparatus for measuring mobile manipulator performance [13]. The apparatus, shown in Figure 3, is called the Reconfigurable Mobile Manipulator Apparatus-1 (RMMA-1). It has a circle pattern of six fiducials and square pattern of four fiducials. The potential for artifacts to be made using three dimensional (3D) printing could lower the cost by perhaps 200 times, as demonstrated through machining costs of the RMMA-1 and the 3D printing of parts used with the artifact.

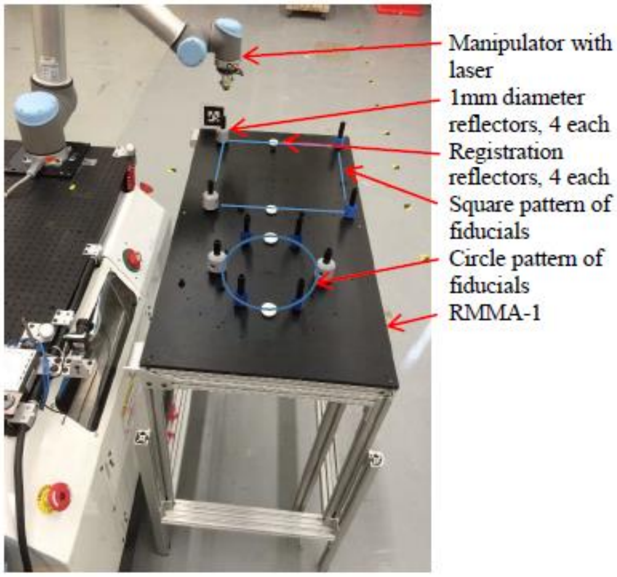

Manipulator with laser
1mm diameter reflectors, 4 each
Registration reflectors, 4 each
Square pattern of fiducials
Circle pattern of fiducials
RMMA-1

Figure 3. RMMA-1 showing circle and square patterns of fiducials for the mobile manipulator to index between.

The test A-UGV can access the artifact from any pose (position and orientation). In [13], a calibrated vehicle carried the onboard manipulator to a point with 5 mm position uncertainty. The manipulator was able to register (determine its position with respect to the artifact) using a circular-spiral search and repeatedly locate 6 mm diameter targets when the manipulator was positioned by the AGV at a static location and next to the square pattern on the RMMA-1.

Recent research [14] demonstrated registration of the mobile manipulator to 1 mm diameter fiducials from any vehicle orientation with respect to the RMMA-1. The registration method incorporated a 0.5 mm step, square-spiral search pattern, and higher resolution A-UGV pose information (0.01 mm position and 0.01° orientation). The research also demonstrated "indexing" between RMMA-1 circle and square patterns as opposed to static positioning of the manipulator at a single pattern. Indexing allows the mobile manipulator to be repositioned to reach each pattern.

A computer aided design model of paths and docking points was used by a vehicle control program to move the A-UGV from one docking point to another. This programming method is inherent in the A-UGV type used. The manipulator control program moves the robot arm from the stowed location to each fiducial and searches for the exact position using a laser retro-reflector detector. The vehicle control program positioned the vehicle at various orientations with respect to the RMMA-1 and the manipulator program corrected for vehicle position and rotation allowing it to quickly find, pre-taught, target registration.

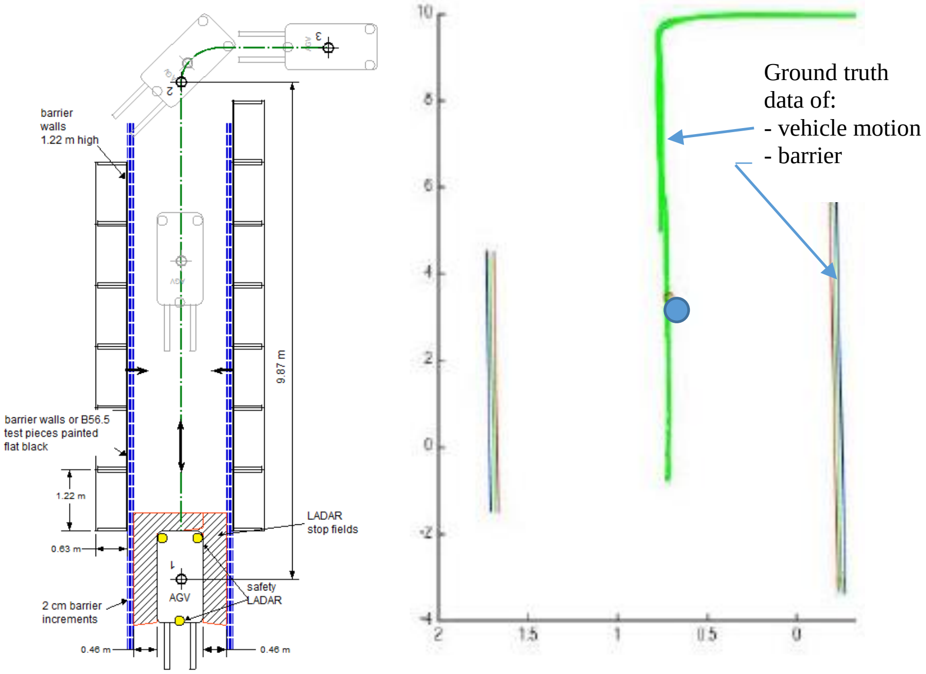
Current research at NIST included a bisecting or "crisscross" search of two large-diameter registration reflectors within each circle and square pattern. Each pattern had a 35 mm and a 30 mm diameter reflector mounted across the pattern edges. The reflectors were detected eight of ten times by the laser retroreflector when perpendicular and pointed at them. The bisecting search concept was to allow the manipulator to rapidly move from the pair of large-uncertainty reflector registration locations to the 1 mm fiducials representing assembly access points. A more refined registration-reflector sizing is a topic for future research. The propagation of manipulator position error will be theoretically examined to optimize the registration speed of mobile manipulators by selection of optimal reflector and search step sizes. As such, using the above explained, relatively inexpensive procedures and apparatus demonstrates a feasible performance measurement test method for mobile manipulators.

4 EXPERIMENTS AND RESULTS

This paper has described new low cost test methods for measuring the performance of A-UGVs. During development, an optical tracking measurement system [14, 15] was used as ground truth. The optical tracker could simultaneously measure the position of all system components. The ground truth system has positional accuracy of 0.02 mm (static) and 0.2 mm (dynamic). The tracking system measured the locations of the vehicle, manipulator, and artifact within the same reference frame. However, more cost-effective means are needed to enable performance tests to be used by A-UGV manufacturers and users. Therefore, the optical tracking system provides verification of the test methods being developed. This section discusses the results of navigation and docking experimental data analysis performed at NIST where several of the tests were initially compared to optical tracking system ground truth for validity while others used only artifacts. The thrust for ASTM F45 performance test methods is the use of replicable and cost effective artifacts.

4.1 Navigation Experiment and Results

The ASTM F45.02 working document navigation test method was constructed using the barriers as shown in Figure 1a. The barrier experimental setup is shown in Figure 4(a) where the A-UGV begins at the lower start point, traverses between the barriers to the top, makes a right turn, stops, and then backs up to the start point. Performance measurement results as compared to the optical tracking ground truth system are shown in Figure 4(b) and show that the A-UGV drove off of the path ± 18 mm.



a

b

Figure 4. a) CAD drawing of navigation test method using barriers. The dotted lines are barrier positions for several tests that reduced the A-UGV corridor width. b) Ground truth measurement data of a navigation test showing (blue circle) the vehicle stop location when barrier detection occurred in the reverse direction. The thicker A-UGV path navigation lines are from different forward and reverse paths.

The measurements demonstrate a need for users and manufacturers of these systems to understand their A-UGV capability and that test methods should be developed that are inexpensive and easily replicated for their use. Figure 4(b) shows results from running the ASTM F45.02 draft test method compared to ground truth.

4.2 Docking Experiments and Results

The navigation sensor [16] for the vehicle used in this research has a manufacturer's stated "best-in-class angle accuracy of 1 mrad (0.057°)". When this specification is applied to the A-UGV navigation sensor distance to the closest reflector, a maximum A-UGV docking uncertainty of 0.5 mm would be expected. However, many factors, such as the location of the navigation sensor relative to the vehicle reference point, wheel wear, and the servo control algorithms, impact the vehicle performance. No manufacturer's vehicle specified performance was provided with the experimental vehicle as is fairly common on industrial vehicles. The following docking experiments were performed and associated results provided.

4.2.1 Vehicle Docking Experiments and Results

Experiments using a fork-style A-UGV and the Docking apparatus shown in Figure 2(b) were performed to measure vehicle docking repeatability. A triangular piece of yellow tape was placed on each fork tip as shown in Figure 2(d). Prior to the experiment the apparatus location was set by moving it to the dock location, since the experiment measured repeatability. The vehicle was programmed with the path as shown in Figure 5 to move forward from home to point 1, stop, and move in reverse with the fork tines pointing at the apparatus. The tines were automatically raised or lowered at stop point 2 to match the chosen apparatus target heights. The vehicle moved to dock with the apparatus at one fork tine height and the next trial moved the tines to the other height. The target heights were set for both upper and lower fork tine positions. Note, to measure vehicle docking accuracy, as opposed to repeatability, the apparatus would have to be placed at a new location whose position is determined independently of the A-UGV and the A-UGV would then be commanded to dock at that position.

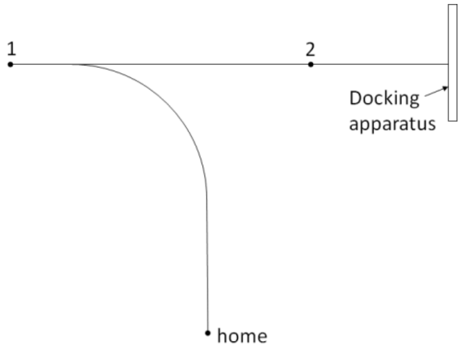


Figure 5. Vehicle path for docking with the apparatus.

The tests were iterated several times with the vehicle moving from a home position to the docking position. The targets measured 76 mm in diameter, which is similar to the height of a pallet opening. Pallet opening widths are much greater than their heights due to their overall pallet widths. Opening widths are typically ½ pallet widths minus their support structure widths (e.g., (1.2 m wide – 0.1 m structure)/2 = 550 mm wide openings). The test results for all iterations showed that the fork tips, marked with the tape points, repeatedly aligned within the approximate 10 mm target centers for both lower- and upper-height white targets, matching experimental results previously determined using the ground truth tracking system. The experimental results demonstrated that the test method provided reproducible docking repeatability results through use of a relatively simple Docking apparatus.

4.2.2 Mobile Manipulator Docking Experiments and Results

The mobile manipulator shown in Figure 3 was used for onboard equipment docking experiments building on previous research [12, 13]. Three recent indexing experiments were performed, as described in section 3.2.2 Vehicle with Onboard Equipment Docking. The three experiments measured 1) detection of 1 mm fiducials used for registration to the artifact, 2) re-registration using detection of two 1 mm fiducials after bisection (crisscross) registration of large reflectors, and 3) repeatability after registration. The main metrics for these tests were success rate and the number of 0.5 mm steps required to detect the first and second points after registration. These metrics are similar to what manufacturers and users may consider when matching a mobile manipulator to assembly tasks. Experiment one docking results after 10 trials using two 1 mm registration fiducials were that the success rate averaged 91 %, although an average of 794 steps in the square-spiral search were required to detect the first assembly point after registration followed by 12 steps to detect the second point.

The re-registration concept, shown in Figure 6, includes a high level reference frame drawing of the system components and crisscross search. The initial bisection search location was measured with the vehicle parked at one of the test locations near both the circle and the square RMMA-1 patterns. The manipulator joystick was then used to jog the manipulator to detect a 1 mm fiducial at the center point where a large reflector was to be placed. The manipulator tool point location was recorded and the search was repeated for all four (two circle and two square) registration point locations. The large reflectors were replaced at the recorded locations and the vehicle was programmed to move to 10 different poses near the RMMA-1 as the manipulator performed the bisection registration. The bisection search used 3 mm steps to rapidly register the large reflector’s center. Large step size on registration reflectors is perhaps one of the greatest uncertainties for this type of registration method, although lower tolerance steps provides much slower registration where a time/tolerance registration balance is a topic for future research.

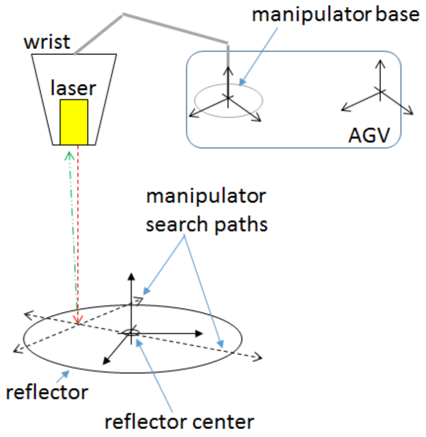


Figure 6. High level reference frame drawing showing the system components and bisection search concept.

The second experiment used the mobile manipulator to do crisscross registration to the RMMA-1 and then to re-register to two 1 mm fiducials. Afterwards, the manipulator was moved to detect the 1 mm fiducials and two more 3 mm fiducials on the square corners and four more on the circle. The experimental goal was to determine if the speed and success rate to detect the second registration were improved from experiment one. The experiment two test results were that success rate was averaged over 10 trials at 92 %. However the number of steps to detect the first and second 1 mm fiducials dropped to an average of approximately 11 steps and 4 steps, respectively. Two of the 10 trials included issues with detecting the large reflectors and were aborted and not included in the results. Future tests with the use of larger reflectors and a smaller, for example 0.5 mm, step search will replace the current large reflectors and 3 mm step search to help remedy this situation. Additionally, improved vehicle pose and manipulator base references will be researched.

The third experiment included the crisscross registration method followed by pattern registration to 1 mm fiducials and then performance measurement of repeatability. The square and the circle were repeated 32 times after registration where registration steps were not included in repeatability tallies. During repeated pattern detection, the success percentage averaged 98 %, detecting two 1 mm and two 3 mm fiducials on the square and two 1 mm fiducials and four 3 mm fiducials on the circle for a total of 1600 points. In all three experiments, the use of artifacts provided reproducible performance measurement methods verifying registration.

5 CONCLUSIONS

ASTM Committee F45 for Driverless Automatic Guided Industrial Vehicles is developing new terms and definitions for the community. The proposed term “A-UGV” provides a single term to span AGV and mobile robot systems. Also, ASTM F45 task groups and the NIST RSSM Program are developing performance test methods for navigation and docking. The navigation test method that is currently near ballot within F45.02 is used to measure an A-UGV's path following accuracy. The navigation test method demonstrates a simple, reproducible, cost effective solution to measure performance of a vehicle traversing, both forward and reverse, a straight path that includes a single turn. Experiments at NIST demonstrated that three different methods defining the path are feasible and useful for measuring navigation performance for A-UGVs.

Similarly, test methods for docking of A-UGVs, both without and with onboard equipment, such as robot arms, will help evaluate vehicle docking capabilities. Performance testing using a vehicle location, laser, and artifacts, such as the Docking artifact and RMMA-1, has proven to be useful and cost effective. Test method experiments at NIST for docking vehicles to an apparatus show repeatable results. Three experiments were performed on the mobile manipulator docking with an apparatus. The results showed that the test method being developed to dock a mobile manipulator with an apparatus provided various registration methods and uncertainties that can be measured using relatively simple and inexpensive components and concepts.

Future tests will be performed increasing the size of the initial reflectors that replace the current large reflectors, as well as improving the vehicle pose and manipulator base references. Also, a new performance artifact called RMMA-2 will be implemented for measuring mobile manipulator performance in dynamic vehicle and manipulator situations (i.e., the base and the arm are simultaneously moving).

6 ACKNOWLEDGEMENTS

The authors would like to thank Sebti Foufou, Qatar University, Doha, Qatar for his guidance on this research and the ASTM F45 task groups for their efforts in developing the terminology and test methods discussed in this paper.

7 REFERENCES

[1] ANSI/ITSDF B56.5:2012, Safety Standard for Driverless, Automatic Guided Industrial Vehicles and Automated Functions of Manned Industrial Vehicles, www.itsdf.org, Nov 2012.

[2] British Standard Safety of Industrial Trucks - Driverless Trucks and their Systems. Technical Report BS EN 1525, 1998.

[3] Robotic Systems for Smart Manufacturing Program, http://www.nist.gov/el/isd/ms/rssm.cfm, National Institute of Standards and Technology, 2016.

[4] "Yaskawa Motoman MH80 robot unloading trucks - from Wynright Corporation," http://www.youtube.com/watch?v=8wngL0BnF_4, June 18, 2013.

[5] Adept Lynx Handler-Semi, http://www.adept.com/products/mobile-robots/mobile-transporters/handler-semi/general, 2016.

[6] ASTM F45 Committee on Driverless Automatic Industrial Vehicles, www.astm.org, 2016.

[7] ASTM F45.91 Terminology subcommittee, work item WK48954, www.astm.org, 2016.

[8] ASTM F45.02 Docking and Navigation subcommittee, work item WK50379, www.astm.org, 2016.

[9] "About Savant Automation", Savant, http://www.agvsystems.com/about/, March 2006

[10] International Standards Organization (ISO) 8373:2011 Robots and robotic devices — Vocabulary

[11] Material Handling Industry of America, Automatic Guided Vehicle Systems, http://www.mhi.org/glossary, 2014.

[12] Roger Bostelman, Tsai Hong, and Elena Messina, "Intelligence Level Performance Standards Research for Autonomous Vehicles", FinE-R 2015 The Path to Success: Failures in Real Robots Workshop, Intelligent Robot Systems (IROS) 2015, Hamburg, Germany, October 2, 2015.

[13] Roger Bostelman, Tsai Hong, Jeremy Marvel, "Performance Measurement of Mobile Manipulators", SPIE 2015, Baltimore, MD, April 2015

[14] Roger Bostelman, Sebti Foufou, Steve Legowik, Tsai Hong Hong, "Mobile Manipulator Performance Measurement Towards Manufacturing Assembly Tasks", 13th IFIP International Conference on Product Lifecycle Management (PLM16), Columbia, SC, July 11-13, 2016.

[15] Roger Bostelman, Joe Falco, Mili Shah, Tsai Hong Hong, "Dynamic Metrology Performance Measurement of a Six Degree-of-Freedom Tracking System Used in Smart Manufacturing", Autonomous Industrial Vehicles: From the Laboratory to the Factory Floor, ASTM Book chapter 7, 2016.

[16] Kollmorgen LS5 product brochure and specification # 35100-154B, www.kollmorgen.com/agv, received March 2016.

Multicast Delayed Authentication For Streaming Synchrophasor Data in the Smart Grid

Sérgio Câmara[1], Dhananjay Anand[2],
Victoria Pillitteri[2], and Luiz Carmo[1]

[1] National Institute of Metrology, Quality and Technology
Duque de Caxias, 25250-020, Rio de Janeiro, Brazil
{smcamara,lfrust}@inmetro.gov.br
[2] National Institute of Standards and Technology
Gaithersburg, MD 20899, USA
{dhananjay.anand,victoria.pillitteri}@nist.gov

Abstract. Multicast authentication of synchrophasor data is challenging due to the design requirements of Smart Grid monitoring systems such as low security overhead, tolerance of lossy networks, time-criticality and high data rates. In this work, we propose *inf*-TESLA, Infinite Timed Efficient Stream Loss-tolerant Authentication, a multicast delayed authentication protocol for communication links used to stream synchrophasor data for wide area control of electric power networks. Our approach is based on the authentication protocol TESLA but is augmented to accommodate high frequency transmissions of unbounded length. *inf*-TESLA protocol utilizes the Dual Offset Key Chains mechanism to reduce authentication delay and computational cost associated with key chain commitment. We provide a description of the mechanism using two different modes for disclosing keys and demonstrate its security against a man-in-the-middle attack attempt. We compare our approach against the TESLA protocol in a 2-day simulation scenario, showing a reduction of 15.82% and 47.29% in computational cost, sender and receiver respectively, and a cumulative reduction in the communication overhead.

Keywords: Multicast authentication, Smart Grid, synchrophasors, Wide Area Monitoring Protection and Control

1 Introduction

Smart Grids are large critical cyber-physical infrastructures and are being transformed today with the design and development of advanced real-time control applications [11]. The installation of Phasor Measurement Units (PMUs) as part of world-wide grid modernization is an example of major infrastructure investments that require secure standards and protocols for interoperability [1].

PMUs take time-synchronized measurements of critical grid condition data such as voltage, current, and frequency at specific locations that are used to provide wide area visibility across the grid.The synchrophasor data aggregated

Camara, Sergio; Anand, Dhananjay; Pillitteri, Victoria; Carmo, Luiz.
"inf-TESLA: Multicast Delayed Authentication For Streaming Sensor Data in Electric Power Systems."
Paper presented at the IFIP Advances in Information and Communication Technology, Ghent, Belgium, May 30-Jun 1, 2016.

from multiple PMUs are used to support real-time analysis, planning, corrective actions, and automated control for grid security and resiliency. Currently, high-speed networks of PMUs are being used for Wide Area Monitoring Protection and Control (WAMPAC) applications to provide situational awareness in the Eastern and Western Interconnection of North America, in China, Canada, Brazil and across Europe [11]. Before the installation of PMUs, the lack of wide-area visibility is one of the factors that prevented early fault identification of the 2003 Northeast America and 2003 Italy blackouts [21] [9]. Malicious PMU data or deliberate attacks could result in inaccurate decisions detrimental to grid safety, reliability, and security, that said, PMUs need information authentication and integrity, while confidentiality may be considered optional.

Authentication schemes in the Smart Grid must be able to efficiently support multicast. Current standard solution, suggested by IEC 62351 [5], comprises HMAC authentication algorithm for signing the synchrophasors. However, sharing only one symmetric key across a multicast group cannot guarantee adequate security, and this approach suffers from the scalability problem. The use of asymmetric cryptography and digital signatures for multicast authentication raises concerns about the impact on cost and microprocessor performance. One-Time Signature schemes can enable multicast authentication, however they suffer from communication and storage overhead, and complicated key management [24].

Although some previous literature works assume, in general, that delayed authentication is not suitable for real-time applications [7] [8], such method is still eligible for some monitoring and control applications that permit relatively larger delay margins (e.g. wide-area oscillation damping control application) [25]. For more considerations on this topic, see Section 2. Moreover, delayed authentication presents advantages over cited issues by supporting multicast data streaming, symmetric and lightweight cryptography, corrupt data and attack detection. Also it allows scalable solutions and key management, tolerates packet loss, and provides low communication overhead and high computational efficiency.

The primary objective of this work is to propose a multicast delayed authentication protocol called *inf*-TESLA in order to provide measurement authentication in a WAMPAC application within the Smart Grid. Also, we design the Dual Offset Key Chains mechanism which is used by our protocol to generate the authenticating keys and to provide long-term communication without the need of key resynchronization between the sender and receivers. A description of two different modes for disclosing keys and a demonstration of a man-in-the-middle attack attempt against out mechanism are also provided.

Section 2 presents an overview of the network architecture used for wide area aggregation of PMU data as well as some delay constraints and authentication infrastructure. In Section 3 we discuss prior work in the area of packet based authentication protocols for streaming communication, and then in Section 4 we present the *inf*-TESLA protocol and describe the Dual Offset Key Chains mechanism along with its security properties and conditions. In Section 5 we evaluate our approach against the original TESLA protocol. Finally, we summarize our results and propose future works in Section 6.

2 Scenario Characteristics

The network architecture considered for this work is as follows. Each communication link in the infrastructure comprises one PMU sender node S capable of multicasting packets to m receivers R_k applications, where $1 \leq k \leq m$. PMU S sends time-stamped synchrophasor data packets at a rate of 10 to 120 packets per second and that can be dropped in the way to the receivers. The network has several n intermediate nodes between S and $R_k, n > 0$, called Phasor Data Concentrators (PDCs). PDCs can chronologically sort received synchrophasors as well as aggregate, repackage and route data packets to the set of higher level PDCs (Super PDCs). When packets are missing or lost, PDCs may (with due indication) interpolate measurements in order to retain the communication link.

There are different wide-area monitoring and control applications that consume synchrophasor data and have different time delays and quality requirements. For instance, Situational Awareness Dashboard, Small-Signal Stability Monitoring, and Voltage Stability Monitoring/Assessment accept up to 500 milliseconds in communication latency, other applications such as Long-term stability control, State Estimation, and Disturbance Analysis Compliance can handle up to 1000 ms. For the entire list, see [20].

Zhu *et al.* [25] simulates the latency for monitoring applications over the Smart Grid network architecture and obtained results within a range of 150–220 ms. For centralized control applications, the latency was well below 500 ms. From the delayed authentication perspective, the minimum delay of the authentication confirmation by R_k is approximately twice the latency of the network. Still, delayed authentication protocols are able to attend the requirements for the above cited applications.

When utilizing multicast communication, IEC 61850-90-5, the standard for communication networks and systems for power utility automation, requires a Key Distribution Center (KDC), which provides the symmetric key coordination between S and R_k. We assume that each S is its own KDC, which is also endorsed by the standard. Furthermore, as our scheme demands that S prove its identity to R_k once during communication initialization, each receiver is required to validate a digital signature from S and maintaining a copy of its public key certificate. For this purpose, we assume that a Public-Key Infrastructure (PKI) is also available.

2.1 Security Considerations

We assume that attacks are accordingly aligned, via a man-in-the-middle, to either manipulate data values or masquerade as a legitimate PMU. Using the attack model from [23], the adversary is not limited by network bandwidth and has full control to drop, resend, capture and manipulate packets. Although his computational resources can be large, it is not unbounded and he cannot invert a pseudorandom function with non-negligible probability. Each receiver R_k is able to authenticate both the content and source of synchrophasor payloads after a delay of d_{NMax} using our delayed authentication scheme presented in Section 4.

However, if a packet fails authentication at time t, then an attack that has been active and undetected since $t - d_{NMax}$ represents the maximum threat exposure.

The security primitives used throughout this paper are as follows:

- *One-way hash function* H operates on an arbitrary length input message M, returning $h = H(M)$. H can be implemented with SHA-2 family algorithms.
- *Message Authentication Code* $MAC(K, M)$ provides a tag that can verify authenticity and integrity of message M given a shared key K. $HMAC(K, M)$ is a specific construction which includes an underlying cryptographic hash function to create the authenticating tag.
- *Hash chain* $H^n(M)$ denotes n successive applications of cryptographic hash function H to message M.

3 Related Work

Multicast authentication is an active research field in recent years and has been applied to a wide range of applications. In Smart Grids, it is being used for monitoring, protection and information dissemination [24]. In this section, we review all the TESLA-based multicast authentication schemes and other multicast authentication schemes used for electrical power systems.

To address the challenge of continuous stream authentication for multiple receivers on a lossy network, Timed Efficient Stream Loss-tolerant Authentication (TESLA) was introduced by Perrig et al [14]. Based on the Guy Fawkes protocol [2] and requiring loose time synchronization between the senders and receivers, TESLA is a broadcast authentication protocol considering delayed disclosure of keys used for authentication of previous sent messages and packet buffering by the receiver. This protocol supports fixed/dynamic packet rate and delivers packet loss robustness and scalability. Benefits of TESLA include a low computation overhead, low per-packet communication overhead, arbitrary packet loss is tolerated, unidirectional data flow, high degree of authenticity and freshness of data. Further work proposed several modifications and improvements to TESLA, allowing receivers to authenticate packets upon arrival, improved scheme scalability, reduction in overhead, and increased robustness to denial-of-service attacks [13].

Studer et al. describe TESLA++ [19], a modified version of TESLA resilient to memory-based DoS attacks. They combine TESLA++ and ECDSA signatures to build an authentication framework for vehicular ad hoc networks.

μTESLA [17] adapts TESLA to make it practical for broadcast authentication in severely resource-constrained environments; like sensor networks. Some of these adaptations include the use of only symmetric cryptography mechanisms, less frequent disclosure of keys and restriction on the number of authenticated senders. Liu and Ning [10] reduce the overhead needed for broadcasting key chain commitments and deal with DoS attacks. Their Multilevel μTESLA protocol considers different levels of key chains to cover the entire lifespan of a sensor.

Other methods include the One-Time Signatures family which gained popularity recently and is applicable to multicast authentication and also for WAMPAC applications. The author in [12] describes a one-time signature based broadcast authentication protocol based on BiBa. BiBa uses one-way functions without trapdoors and exploits the birthday paradox to achieve security and verification efficiency. Its drawbacks include a large public key and high overhead for signature generation.

HORS [18] is described by Reyzin et al. as an OTS scheme with fast signing and signature verification using a cryptographic hash function to obtain random subsets for the signed message and for verifying it, but it still suffers from frequent public key distribution. TSV [8] multicast authentication protocol generates smaller signatures than HORS and has lower storage requirement at the cost of increased computations in signature generation and verification. TSV+ [7], a patched version of TSV, uses uniform chain traversal and supports multiple signatures within an epoch. SCU [22] is a multicast authentication scheme designed for wireless sensor networks and SCU+ [7] adapts it for power systems using uniform chain traversal as well. TV-HORS [23] uses hash chains to link multiple key pairs together to simultaneously authenticate multiple packets and improves the efficiency of OTS by signing the first l bits of the hash of the message. As a downside, TV-HORS has a large public key of up to 10 Kbytes.

4 Proposed Solution

In this section, we propose *inf*-TESLA, a new TESLA based scheme that improve its overall performance. At first, we review TESLA to give some background and then present our scheme.

4.1 TESLA

Timed Efficient Stream Loss-tolerant Authentication (TESLA) [14] [13] [15] [16] is a broadcast authentication protocol with low communication and computation overhead, tolerates packet loss and needs loose time synchronization between the sender and the receivers.

TESLA relies on the delayed disclosure of symmetric keys, therefore the receiver must buffer the received messages before being able to authenticate them. The keys are generated as an one-way chain and are used and disclosed in the reverse order of their generation. At setup time, the sender must first set n as the index of the first element K_n. For generating the key chain, the sender picks a random number for K_n and using a pseudo-random function f, he constructs the one-way function $F : F(k) = f_k(0)$. So, the sender generates recursively all the subsequent keys on the chain using $K_i = F(K_{i+1})$. By that, the last element of the chain is $K_0 = F^n(K_n)$, and all other elements could be calculated using $K_i = F^{n-i}(K_n)$.

Each K_i looks pseudo-random and an adversary is unable to invert F and compute any K_j for $j > i$. In the case of a lost packet containing K_i, a receiver can calculate K_i given any subsequent packet containing K_j, where $j < i$, since $K_j = F^{i-j}(K_i)$. As a result, TESLA tolerates sporadic packet losses.

The stream authentication scheme of TESLA is secure as long as the security condition holds: A data packet P_i arrived *safely*, if the receiver can unambiguously decide, based on its synchronized time and maximum time discrepancy, that the sender did not yet send out the corresponding key disclosure packet P_j.

TESLA also supports both communication with fixed or dynamic packet rate. For fixed rate, the sender discloses the key K_i of the data packet P_i in a later packet P_{i+d}, where d is a delay parameter set and announced by the sender during setup phase. The sender determines the delay d according to the packet rate r, the maximum tolerable synchronization uncertainty δ_{tMax} and the maximum tolerable network delay d_{NMax}, setting $d = \lceil(\delta_{tMax} + d_{NMax})r\rceil$. In this mode, the scheme can achieve faster transfer rates. For dynamic rate, the sender pick one key per time interval T_{int}. Each key is assigned to a uniform interval of duration T_{int}, T_0, T_1 ,..., T_n, that is, key K_i will be active during the time period T_i. The sender uses the same key K_i to compute the MAC for all packets which are sent during T_i, on the other hand, all packets during T_i disclose the key $K_{i-d'}$. In this case, $d' = \lceil(\delta_{tMax} + d_{NMax})/T_{int}\rceil$. We use the designation d and d' for fixed and dynamic rates respectively.

For each new receiver that joins the communication network, the sender initially creates an authenticated synchronization packet. This packet contains parameters such as interval information, the disclosure lag and also a disclosed key value - which is a commitment to the key chain. The sender digitally signs this packet to each new receiver before starting the streaming communication.

4.2 *inf*-TESLA

inf-TESLA, short for infinite TESLA, is a multicast authentication protocol based on TESLA suitable for use in long term communication at high packet rates. As in TESLA, *inf*-TESLA relies on the strength of symmetric cryptography and hash functions and on the delayed disclosure of keys as a means to authenticate messages from the sender. Also, it requires only loose time synchronization between the sender and the receiver and can operate under both dynamic and fixed packet rates.

By using fixed packet rate mode, there is no need for setting specific time intervals for MACing and disclosing keys. Each autheticating key is used once for the actual message and disclosed d packets later. Although this operational mode can achieve maximum speed on authenticating previous packets, it has a drawback of quickly consuming the authenticating key chain, depending on the frequency of the packets.

Since we use one-way hash functions to build independent key chains, every time one of the key chains comes to an end (meaning that it was fully used in the authentication process) the sender must automatically build, store and utilize a new key chain in its place. In the original TESLA protocol, a sender would have to reassign a new synchronization packet as the current key chain comes to an

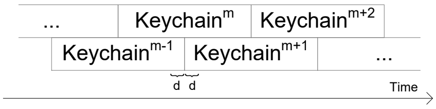


Fig. 1. An illustration of dual offset key chains as used for *inf*-TESLA.

end, inflicting non-negligible network and computational overhead by digitally signing a synchronization packet at the end of each key chain.

inf-TESLA addresses this issue by using the Dual Offset Key Chains mechanism. This mechanism uses a pair of keys for each message and guarantees continuity of the multicasting authentication process without the need for signing and sending a new synchronization packet. The mechanism creates two offset key chains so that a pair of active key chains are always available and, as the main principle, a key chain m always straddles the substitution of key chain $m-1$ with $m+1$. Figure 1 illustrates the Dual Offset Key Chains mechanism by which key chain m supports the substitution of key chain $m-1$ for key chain $m+1$ without the need for resynchronization. A detailed description of the Dual Offset Key Chains mechanism is presented on Section 4.2.

The overall initialization setup is similar to TESLA. Before the data streaming begins, the sender first determines some fundamental information about the network status, d_{NMax}), and time synchronization, δ_{tMax}, and builds its first two key chains. We assume that both sender and receiver are time synchronized by a reliable time protocol (e.g. PTP). After that, the sender S chooses the delay parameter d (Section 4.1) that will base the decision of the receiver R_k to either accept a packet from S. This condition is **Security Condition-1** for *inf*-TESLA.

For bootstrapping each new receiver, S constructs and sends the synchronization (commitment) packet to the new incomer. For a dynamic packet rate, this packet contains the following data [13]: the beginning time of a specific interval T_j along with its id I_j, the interval duration T_{int}, the key disclosure delay d', a commitment to the key chain K_i^m and key chain K_i^{m+1} ($i < j - d'$ where j is the current interval index).

For a fixed packet rate r, let j_1 and j_2 be the current key from key chains m and $m+1$ respectively. The synchronization packet contains: delay d and the commitment for the key chains $K_{i_1}^m$ and $K_{i_2}^{m+1}$ ($i_1 < j_1 - d$ and $i_2 < j_2 - d$). We will focus on fixed packet rate in this paper for the sake of brevity and convenience of notation. While a fixed packet rate is potentially more likely for the streaming applications we address, our approach is compatible with both dynamic and fixed rates.

Dual Offset Key Chains mechanism. The Dual Offset Key Chains mechanism enables continuity in streaming authentication without the periodic resynchronization between S and $R_k \in R$ required by TESLA. Two key chains, offset in alignment, are used simultaneously by the mechanism to authenticate messages. For every packet, there are always two active key chains and, from each chain, one non-used key available for MACing.

For constructing the two key chains, first the sender chooses n, the total number of elements on a single key chain. Let l^m be the current number of remaining elements on the key chain m. Here we assume that all created keys are deleted just after being used for authenticating messages. Let M be the maximum available memory for storing the key chains, assuming that M is big enough for storing two key chains, m and $m+1$, at any time. The value of n must be chosen accordingly to the following constraints: (i) $n \geq l^{m-1} + 2(d+1)$ and (ii) $n \leq \frac{M}{2} + d$.

The the first constraint sets a minimum value for n, that is the minimum initial size of a key chain. During the initialization setup of the first receiver synchronization, we consider $l^{m-1} = 0$ for constructing the first key chain. The second constraint restricts the maximum number of elements in a key chain. If a key chain m does not meet this limit, key chain $m+1$ will not be long enough to meet the security condition for the key chain exchange procedure (see Section 4.2). In practice, it may not be feasible to calculate a whole key chain in the time taken to send two data packets and so S may compute and store key chain $m+1$ well before the end of key chain $m-1$.

A packet P_j sent by S is formed by the following data $P_j = \{M_j, i_1, i_2, K^m_{i_1-d}, K^{m+1}_{i_2-d}, MAC(K^m_{i_1} || K^{m+1}_{i_2}, M_j)\}$. Every packet carries the actual message M_j, the current sequence number of each key chain i_1 and i_2, the disclosed authenticating keys $K^m_{i_1-d}$ and $K^{m+1}_{i_2-d}$ (discussed later in Section 4.2) and the MAC of the message resultant from an operation that uses the concatenation of current keys from both key chains. In particular, at the beginning of a key chain K^m, the notation K^m_{i-d} may refer to the last keys in the key chain K^{m-1}.

Disclosure of keys. *inf*-TESLA has two modes of operation for disclosing keys: **2-keys** and **Alternating**. In the 2-keys mode (or standard mode, as previously described), each packet P_j discloses two authentication keys, one from each key chain, for the same message M_i, that is packet P_j has the following information, $P_j \rightarrow K^m_{i_1}, K^{m+1}_{i_2}$.

The Alternating mode discloses one key from each key chain alternatively in each data packet. Formally, two consecutive packets would have the following information about keys, $P_j \rightarrow K^m_{i_1}$ and $P_{j+1} \rightarrow K^{m+1}_{i_2+1}$, where indexes i_1 and i_2 correspond to the keys of both key chains to be disclosed in the same data packet in 2-keys mode of operation. Figure 2 shows the key chains in time and the two modes for disclosing keys. In Section 5, we present a more detailed comparison of these two modes in relation to communication overhead, computational cost and authentication delay.

The disclosure delay d for the keys is directly affected by the maximum tolerable network delay d_{NMax}, so each receiver R_k will present a different delay value. Sender S must set d as the largest expected delay in order to meet security condition-1.

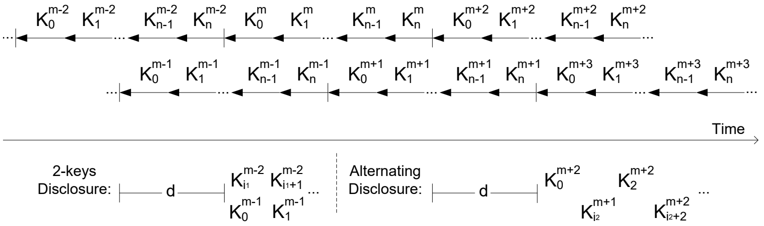

K_0^{m-2} K_1^{m-2} K_{n-1}^{m-2} K_n^{m-2} K_0^{m} K_1^{m} K_{n-1}^{m} K_n^{m} K_0^{m+2} K_1^{m+2} K_{n-1}^{m+2} K_n^{m+2}
K_0^{m-1} K_1^{m-1} K_{n-1}^{m-1} K_n^{m-1} K_0^{m+1} K_1^{m+1} K_{n-1}^{m+1} K_n^{m+1} K_0^{m+3} K_1^{m+3} K_{n-1}^{m+3} K_n^{m+3}
Time
2-keys Disclosure:
d
$K_{i_1}^{m-2}$ $K_{i_1+1}^{m-2}$ ...
K_0^{m-1} K_1^{m-1}
Alternating Disclosure:
d
K_0^{m+2} K_2^{m+2} ...
$K_{i_2}^{m+1}$ $K_{i_2+2}^{m+2}$

Fig. 2. Two modes for disclosing keys: 2-keys and alternating.

Dual Offset Key Chains mechanism security. Key chain security is based on the widely used cryptographic primitive: the one-way chain. One-way chains were first used by Lamport for one-time password [6] and has served many other applications in the literature.

The **Security Condition-2** for *inf*-TESLA concerns the key chain exchange procedure. This condition states that both key chains cannot be substituted within a time interval d/r (or within d packets). If this happens, the receiver must drop the following packets and request for resynchronization with the sender. This protocol restriction assures the authentication inviolability of *inf*-TESLA and must be observed at all times by the receiver. The receiver is solely responsible for monitoring the key chain exchange procedure and accepting, or rejecting, the new key chain.

In Figure 3, we show an example of a man-in-the-middle attack attempt on the Dual Offset Key Chains mechanism and the importance of the security condition-2. For this example, we consider $d = 9$ as minimum number packets the sender has to wait to disclose a key, the last element $n = 50$ for all key chains, and the asterisk symbol indicates an item maliciously inserted by the attacker. The packets are presented without indices "i" for cleaner presentation.

We first illustrate how this attack can work on a single key chain mechanism without commitment packets as follows: When the attacker senses a change in the key chain by testing every disclosured key *(a)*, he inserts M_0^* as the first manipulated message and MACs it using the first element K_0^* of a forged key chain of his own. The attacker continues faking the messages and its MACs till the last authentic key used for MACing is disclosured. After that point, the attacker is able to take complete control of the communication without being detected (b). For the second part of Figure 3, the same attack is attempted against our mechanism. Also the attacker is able to sense when a disclosured key chain comes to an end and can also substitute the messages and the MACs in the packets. However, when he tries to take complete control of the key chain by forcing the forged key K_0^{**} over the key chain $m = 2$, this indicates for the receiver a violation of the security condition-2 for the key chain exchange procedure.

Another concern is how many consecutive packets could be lost by the receiver without actually being an attack. Following the security condition for key chain substitution, there must not be two different key chain substitutions

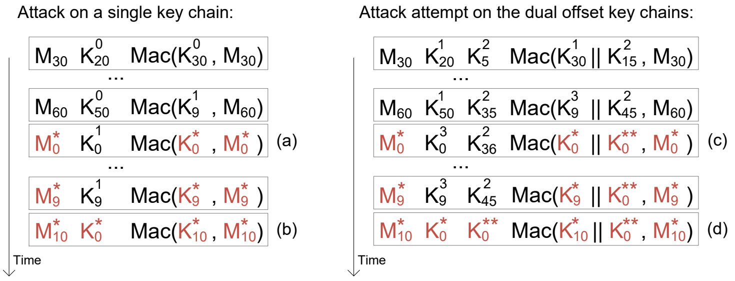

Attack on a single key chain:
M_{30} K^0_{20} Mac(K^0_{30}, M_{30})
...
M_{60} K^0_{50} Mac(K^1_9, M_{60})
M^*_0 K^1_0 Mac(K^*_0, M^*_0) (a)
...
M^*_9 K^1_9 Mac(K^*_9, M^*_9)
M^*_{10} K^*_0 Mac(K^*_{10}, M^*_{10}) (b)
Time
Attack attempt on the dual offset key chains:
M_{30} K^1_{20} K^2_5 Mac(K^1_{30} || K^2_{15}, M_{30})
...
M_{60} K^1_{50} K^2_{35} Mac(K^3_9 || K^2_{45}, M_{60})
M^*_0 K^3_0 K^2_{36} Mac(K^*_0 || K^{**}_0, M^*_0) (c)
...
M^*_9 K^3_9 K^2_{45} Mac(K^*_9 || K^{**}_0, M^*_9)
M^*_{10} K^*_0 K^{**}_0 Mac(K^*_{10} || K^{**}_0, M^*_{10}) (d)
Time

Fig. 3. Example of a man-in-the-middle attack on a single hash chain without commitment and on the Dual Offset Hash Chains mechanism.

within a period of d/r, so the receiver must be aware that the limit for consecutive packets lost is at maximum d. If, for some reason, more than d packets are lost/dropped, the receiver must assure that the following disclosed keys are authentic elements of at least one of the existing key chains, otherwise the receiver will not be able to authenticate any of the next received packets. From this point, the receiver must refuse this stream and request for a new synchronization with the sender.

Another security issue can occur when the last key K_n in the key chain's sequence is lost, that can cause a total lack of authentication of a previous packet P_n. When some K_i is lost, it can be computed from any subsequent key in the key chain through function F (Section 4.1), however when $i = n$ there is no subsequent key. This issue can be extended for the last d elements of the key chain, meaning that in this scenario some packets may not be authenticated and then must be dropped by the receiver. For the Alternating mode for disclosing keys, the receiver would drop $d+1$ packets in the worst case. This issue concerning the last keys of the key chain is a vulnerability of the original TESLA as well.

Elaborate attacks, like selective drop of packets, can cause even more authentication delay without being noticed. For instance, in the case of the Alternating keys disclosure mode, one attacker can induce an alternating drop of packets preventing the sender to authenticate some sequential packets. To mitigate these attacks, the receiver must set an upper limit for the maximum number of non authenticated packets to ignore before resynchronizing with the sender.

5 Evaluation against TESLA

For the following comparison evaluation, we check for communication overhead, authentication delay and computational cost on a long term communication for each of the following schemes: original TESLA, *inf*-TESLA 2-keys (two disclosured keys per packet) and *inf*-TESLA alt (alternating key chain disclosure). Due to PMUs' operational settings, we are only considering a fixed packet rate mode. Also, we assume the following constraints for the simulation:

Table 1. Communication overhead.

	Formula
TESLA (fixed)	$C * (sKey + sSig) + P * (sKey + sMac)$
Inf-TESLA 2-keys	$2 * sKey + sSig + P * (2 * sKey + sMac)$
Inf-TESLA alt	$2 * sKey + sSig + P * (sKey + sMac)$
	2-day simulation (MBytes)
TESLA (fixed)	331,825
Inf-TESLA 2-keys	497,664
Inf-TESLA alt	331,776

- Phasor data frame size of 60 bytes, according to the C37.118 standard [25], over UDP transport layer protocol.
- Pseudo-Random function and HMAC function implementation as HMAC-SHA-256-128. Both HMAC key size and HMAC tag size (truncated) of 128 bits.
- Digital signature implemented as ECDSA over GF(p) of 256 bits. Although TESLA considers RSA signatures, for comparison purposes we use ECDSA signatures. The keys and signatures sizes are based on the NIST SP 800-131A [3] for recommendations on use of cryptographic algorithms and key lengths.
- Maximum number of keys n that can be stored at a time in the cache memory of a device is 10,000 keys.
- Sender's packet rate (frequency) of 60 packets/sec.
- Simulation testing time of 2 days. Past references [7] established a baseline of 1024 key chains for evaluating the one-time signature multicast schemes. However, as *inf*-TESLA must build approximately 4 times the number of key chains as TESLA for the same number of packets, comparisons are done for fixed simulation duration rather than number of key chains.

Table 1 shows the formulas to calculate all security related communication overhead of each of the 3 schemes. Let C be the number of commitments (signed packets), P the total number of transmitted packets and $sKey$, $sMac$ and $sSig$ be the size of a cryptographic key, the size of the MAC tag and the size of a signature tag respectively. *inf*-TESLA 2-keys presents the higher communication overhead due to two disclosed keys per packet, while TESLA and *inf*-TESLA alt present a slightly, but negligible, difference on the overhead during two days of communication.

For calculating the computational cost overhead of each scheme, we use the formulas shown in Table 2. The processing cost in cycles per each operation of hashing, macing, signing and verifying is represented by $cHash$, $cMac$, $cSig$ and $cVer$ respectively. From the graph in Figure 4, we can observe the higher computational cost of the sender and receiver operating TESLA over *inf*-TESLA, due to constant signing and verification operations.

For two days of simulation in this configuration, a sender running TESLA protocol on fixed packet rate mode has to sign up to 1036 commitment packets and spends on average 0.373117 gigacycles/hour, while running *inf*-TESLA he would spend 0.314087 gigacycles/hour of operation, which means a reduction

Table 2. Computational cost calculation.

	Sender
TESLA (fixed)	$C * cSig + P * (cMac + cHash)$
Inf-TESLA (both)	$cSig + 2 * P * (cMac + cHash)$
	Receiver
TESLA (fixed)	$C * cVer + P * (cMac + cHash)$
Inf-TESLA (both)	$cVer + 2 * P * (cMac + cHash)$

of 15.82% in computational cost for the sender. On the receiver side, a TESLA receiver spends in average 0.596289 gigacycles/hour, while *inf*-TESLA needs 0.314303 gigacycles/hour, meaning a reduction of 47.29% in computational cost for the receiver. All values of cycles/operation of the security primitives are referenced from the Crypto++ Library 5.6.0 Benchmarks [4].

Although the alternating keys disclosure mode showed good results on the two previous evaluations, this mode increases the authentication delay of a packet P_i by one packet. That is because the second key needed for authenticating P_i, i.e. $K_{i_2}^{m+1}$, will only be disclosed on P_{j+1} where $j > i + d$. Also, if P_{j+1} happens to be lost, the authentication of P_i will be only achieved when receiver has the disclosed key included in P_{j+3}. On both other schemes, the authentication of a packet P_i is normally achieved after receiving P_j, $j > i + d$, and if P_j is lost, the missing keys can be recovered from the contents in P_{j+1}. Also regarding authentication delay evaluation, necessary time overhead for generation and verification of digital signatures during key chains exchange may affect TESLA's continuous flow on higher frequencies of streamed data.

Although TESLA protocol is an efficient protocol and has low security overhead, it was not originally designed for long-term communication. We observe that *inf*-TESLA, in alternating disclosure mode, can deliver a slightly lower

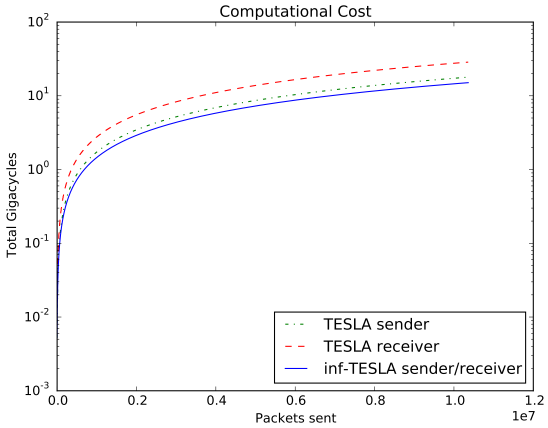


Fig. 4. Computational cost for TESLA and *inf*-TESLA over 2 days of streaming data.

communication overhead and, for both modes, result in a significant reduction in computational overhead over the original protocol. In general, *inf*-TESLA scheme also provides great suitability for key storage and computational constrained devices, such as in Wireless Sensor Networks (WSNs).

6 Conclusion

In this work, we present *inf*-TESLA, a multicast delayed authentication protocol for streaming synchrophasor data in the Smart Grid, suitable for long-term communication and high data rates scenarios. To authenticate messages from the sender, *inf*-TESLA uses two keys to generate the MAC of the message and discloses both keys after a time frame d/r, on a fixed packet rate of operation.

We also design the Dual Offset Key Chains mechanism to produce the authenticating keys and provide a long-term communication without the need of frequently signing resynchronization packets containing commitments to the new key chains, which ensures continuity of the streaming authentication. We prove our mechanism against a man-in-the-middle attack example and describe the security conditions that must be observed at all times by the receiver. *inf*-TESLA enables two different modes for disclosing keys, 2-keys (or standard) and Alternating keys. We present a comparison between this two modes against TESLA within a WAMPAC application, and our protocol shows even more efficiency when compared to the original. Although the Alternating key disclosure mode increases the authentication delay by one packet, it provides less impact on communication overhead and a reduction of 15.82% and 47.29%, sender and receiver respectively, in computational cost during operational time. Generally, *inf*-TESLA shows promise and suitability for key storage and computational constrained devices.

In future work, we intend to do a further analysis on the trade-off between key storage size in devices and protocol performance, and on the possible (minimum/maximum/average) values for the authentication delay by simulating our protocol in a WAMPAC network.

References

1. Greer et al., C.: NIST Framework and Roadmap for Smart Grid Interoperability Standards. Tech. rep., NIST (2014)
2. Anderson, R., Bergadano, F., Crispo, B., Lee, J.H., Manifavas, C., Needham, R.: A new family of authentication protocols. ACM SIGOPS Operating Systems Review 32, 9–20 (1998)
3. Barker, E., Roginsky, A.: Recommendation for transitioning the use of cryptographic algorithms and key lengths. SP 800-131A Transitions (2011)
4. Dai, W.: Crypto++ 5.6. 0 benchmarks. Website at http://www.cryptopp.com/benchmarks.html (2009)
5. International Electrotechnical Commission: IEC TS 62351-1 Power systems management and associated information exchange - Data and communications - Part 1: Communication network and system security-Introduction to security issues (2007)

6. Lamport, L.: Password authentication with insecure communication. Communications of the ACM 24(11), 770–772 (1981)
7. Law, Y.W., Gong, Z., Luo, T., Marusic, S., Palaniswami, M.: Comparative study of multicast authentication schemes with application to wide-area measurement system. Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security p. 287 (2013)
8. Li, Q., Cao, G.: Multicast authentication in the smart grid with one-time signature. IEEE Transactions on Smart Grid 2, 686–696 (2011)
9. Liscouski, B., Elliot, W.: Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations. A report to US Department of Energy 40(4) (2004)
10. Liu, D., Ning, P.: Multilevel μTESLA: Broadcast Authentication for Distributed Sensor Networks. ACM Trans. Embed. Comput. Syst. 3, 800–836 (2004)
11. Patel, M., Aivaliotis, S., Ellen, E.: Real-time application of synchrophasors for improving reliability. NERC Report, Oct (2010)
12. Perrig, A.: The BiBa one-time signature and broadcast authentication protocol. Proceedings of the 8th ACM conference on Computer and Communications Security p. 28 (2001)
13. Perrig, A., Canetti, R., Song, D.: Efficient and secure source authentication for multicast. Proceedings of the Internet Society Network and Distributed System Security Symposium pp. 35–46 (2001)
14. Perrig, A., Canetti, R., Tygar, J.D., Song, D.: Efficient Authentication and Signing of Multicast Streams over Lossy Channels. Proceedings of the IEEE Symposium on Security and Privacy 28913, 56–73 (2000)
15. Perrig, A., Canetti, R., Tygar, J., Song, D.: The TESLA broadcast authentication protocol. CryptoBytes Summer/Fall, 2–13 (2002)
16. Perrig, A., Song, D., Canetti, R., Tygar, J., Briscoe, B.: Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction. The Internet Society RFC:4082, 1–22 (2005)
17. Perrig, A., Szewczyk, R., Tygar, J., Wen, V., Culler, D.E.: Spins: Security protocols for sensor networks. Wireless networks 8(5), 521–534 (2002)
18. Reyzin, L., Reyzin, N.: Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying. Information Security and Privacy 2384, 1–47 (2002)
19. Studer, A., Bai, F., Bellur, B., Perrig, A.: Flexible, extensible, and efficient VANET authentication. Journal of Communications and Networks 11, 574–588 (2009)
20. Tuffner, F.: Phasor Measurement Unit Application Data Requirements. Tech. rep., Pacific Northwest National Laboratory (2014)
21. UCTE: Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy. Tech. Rep. April, Union for the Coordination of the Transmission of Electricity (2004)
22. Ugus, O., Westhoff, D., Bohli, J.M.: A rom-friendly secure code update mechanism for wsns using a stateful-verifier τ-time signature scheme. In: Proceedings of the second ACM conference on Wireless network security. pp. 29–40. ACM (2009)
23. Wang, Q., Khurana, H., Huang, Y., Nahrstedt, K.: Time valid one-time signature for time-critical multicast data authentication. Proceedings - IEEE INFOCOM pp. 1233–1241 (2009)
24. Wang, W., Lu, Z.: Cyber security in the Smart Grid: Survey and challenges. Computer Networks 57(5), 1344–1371 (April 2013)
25. Zhu, K., Nordstrom, L., Al-Hammouri, A.: Examination of data delay and packet loss for wide-area monitoring and control systems. In: Energy Conference and Exhibition (ENERGYCON), 2012 IEEE International. pp. 927–934 (Sept 2012)

Measuring the Effect of Wireless Sensor Network Communications on Industrial Process Performance

Richard Candell, Kang Lee

National Institute of Standards and Technology, Gaithersburg MD, U.S.A
richard.candell@nist.gov

Abstract — Real-time sensor data is essential for making decisions in controlling industrial processes. Wireless sensor networks (WSN's) are becoming more common for industrial processes and condition monitoring. However, wireless communication is subject to interference and thus may affect critical industrial operations. A wireless testbed was developed to study how various wireless sensor network configurations and topologies affect the performance and safety of manufacturing plant operations. A continuous process chemical plant operation was adopted and run in simulation. The chemical process adopted is the Tennessee Eastman Challenge Process with the Lawrence Ricker decentralized controller. The simulated process with sensor output is interfaced to an IEEE 802.15.4-based wireless sensor network via a programmable logic controller (PLC). This integration of the simulated physical system with a real wireless network allows us to examine the effects of real-time wireless communications in a factory running different wireless activities on simulated plant processes. This paper describes the testbed and presents preliminary results of the study.

Keywords — wireless sensor network, wireless control, chemical process, cybersecurity, industrial security, process control, radio environment emulation, chemical process simulation, hardware-in-the-loop, HIL, IEEE 802.15.4, WirelessHART, ISA100.11a, Industrial IoT, SCADA

I. Motivation

The Industrial Internet of Things (IIoT) has introduced a variety of economic advantages to the manufacturing industry. These advantages are based on the increased ability to sense the physical systems and correlate the data to improved efficiencies in production. The IIoT promises manufacturers the ability to monitor and control their processes in real-time with increased operational efficiency and uptime, improved visibility into factory operations, and collaboration between humans and machines thus improving productivity and work experiences [1]. These economic advantages have spurred rapid production of wireless sensing devices for use in industrial environments [2]; however, most of these devices are designed for sensing and few offerings exist for wireless actuation. A prevailing opinion of wireless networks is that the presumed reliability issues of wireless communications make wireless control a non-starter for most manufacturers. In addition, wireless is often presumed to be less secure than that of the wired alternatives. Using a measurement science approach, our wireless testbed is designed to investigate the effectiveness and security of wireless technologies when applied to sensing and control. The results of our study will be used to inform a set of guidelines that will support manufacturers in the use of wireless sensing technologies in their industrial automation systems.

II. Wireless Technology for Process Control

Over the last two decades, many wireless technologies have emerged for use in office and home environment. These technologies include the ubiquitous Wi-Fi™ which is based on the IEEE 802.11 standards. The primary objective of the 802.11 standards was wireless connectivity between home and office computers and a router that enabled users to access internet resources while maximizing throughput within a finite channel bandwidth. This approach to wireless networking has been very successful for applications that can tolerate multiple access channel contention and indeterminate packet flight time. Cases do exist where IEEE 802.11 wireless networks are used for industrial application, and those applications typically focus on a shared communication medium for sensor instrumentation, push-to-talk voice, and video surveillance. Indeed, for applications that require packet arrival determinism and reliability, the IEEE 802.11 standards may be sufficient in some case and insufficient in others [3]. IEEE 802.11 technologies have been gradually applied for various industrial plant process applications that involve real-time transfer of data and voice, position location, and video streaming. An example of this is the application of the 802.11 layer 2 wireless technology based on peer-to-peer mobile ad-hoc network (MANET) at a cement factory located in Chicago, Illinois and in another cement factory in Hagerstown, Maryland [4].

In 2003, the IEEE 802.15.4 standard emerged to address the need for reliable wireless communications that may be used in industrial applications. The standard could fill an important role in the industrial internet of things (IIoT). The IEEE 802.15.4 standard of wireless communications provides a lightweight physical and link layer protocol for low power devices. Many higher-layer protocols now exist to make IEEE 802.15.4 easier to apply to industrial applications. These protocols include ISA 100.11a (IEC 62734) [5], WirelessHART (IEC 62591) [6], and ZigBee [7]. Each of these protocols are similar in that IEEE 802.15.4 is used at the lowest layers with differences appearing in their higher-layer approaches to network architecture routing[8], security[9], and application interfaces.

III. Chemical Reactor Process Description

A chemical reactor is an example of industrial system involving many measured and manipulated variables. One such available model of a chemical reactor process is the Tennessee Eastman (TE) process model defined in [10]. The TE process model is illustrated in Figure 1. This model was chosen for a number of reasons. First, the TE model is a well-known plant model used in control systems research and the dynamics of the plant process are well-understood [11]. Second, the process must be controlled;

otherwise, perturbations will drive the system into an unstable state. By being open-loop unstable, the TE process model represents a real-world scenario in which a communications reliability event could pose an appreciable risk to human safety, environmental safety, and economic viability. Third, the process is complex, highly non-linear, and has many degrees of freedom by which to control and perturb the dynamics of the process. And finally, numerous simulations of the TE process have been developed and reusable code is readily available. We chose to use the controller developed by Lawrence Ricker of the University of Washington [12]. The Ricker Simulink model was chosen for its multi-loop control architecture making distributed control architectures viable. The physical process is described by Downs and Vogel (D&V) in detail in [10], however, a synopsis is given in the following paragraphs.

D&V did not reveal the actual substances used in the process, but instead used generic identifiers for each. The process produces two products, G and H from four reactants A, C, D, and E. The process is defined as irreversible and exothermic, and the reaction rates of the four reactants are a function of the reactor temperature. The process is broken into five major operations, which include a reactor, a product condenser, a vapor-liquid separator, a product stripper, and a recycle compressor.

Gaseous reactants are combined in the reactor to form liquid products. The reactor temperature must be controlled and is cooled using cold water cooling bundles. The reaction is not 100 % efficient and some gaseous feed components remain. The output of the reactor is fed to a condenser where the products are further cooled into liquid form. The vapor-liquid separator then separates unreacted gases from the liquid products. The unreacted gases are sent back to the reactor by a centrifugal recycle compressor. Again, the separation process is not 100 % efficient, and the remaining reactants are removed in a stripping column by stripping the mixture with C in feed stream four (4). The products, G and H, are then sent downstream for further refining. Byproducts of the process are purged from the process through the purge valve of stream nine (9).

The process has six (6) different modes of operation, which control the G/H mass ratio and the production rate through stream eleven (11). Our primary use case for the system is the base case indicated as Mode 1. D&V provided heat and material balance data for the Mode 1 case. It is important to note that the process is designed to shut down if the reactor pressure exceeds 3000 kPa; however, as noted in [2] the reaction efficiency improves as reactor pressure increases. This indicates that reactor pressure must be driven as close to the maximum threshold without exceeding the shutoff limit. The reactor pressure therefore represents a vulnerability to system integrity [11] that could be induced through a security breach or a network reliability problem. It is conceivable that the network could be compromised by radio frequency (RF) interference or a change in the RF environment (e.g. the addition of a physical structure that adversely impacts electromagnetic propagation). Krotofil and Cardenas provide an excellent discussion of how security vulnerabilities affect the physical performance of the TE process [13]. These security vulnerability impacts are analogous to wireless communications impacts on process performance. Our research here measures the impact of wireless communications on the performance of the chemical reaction process.

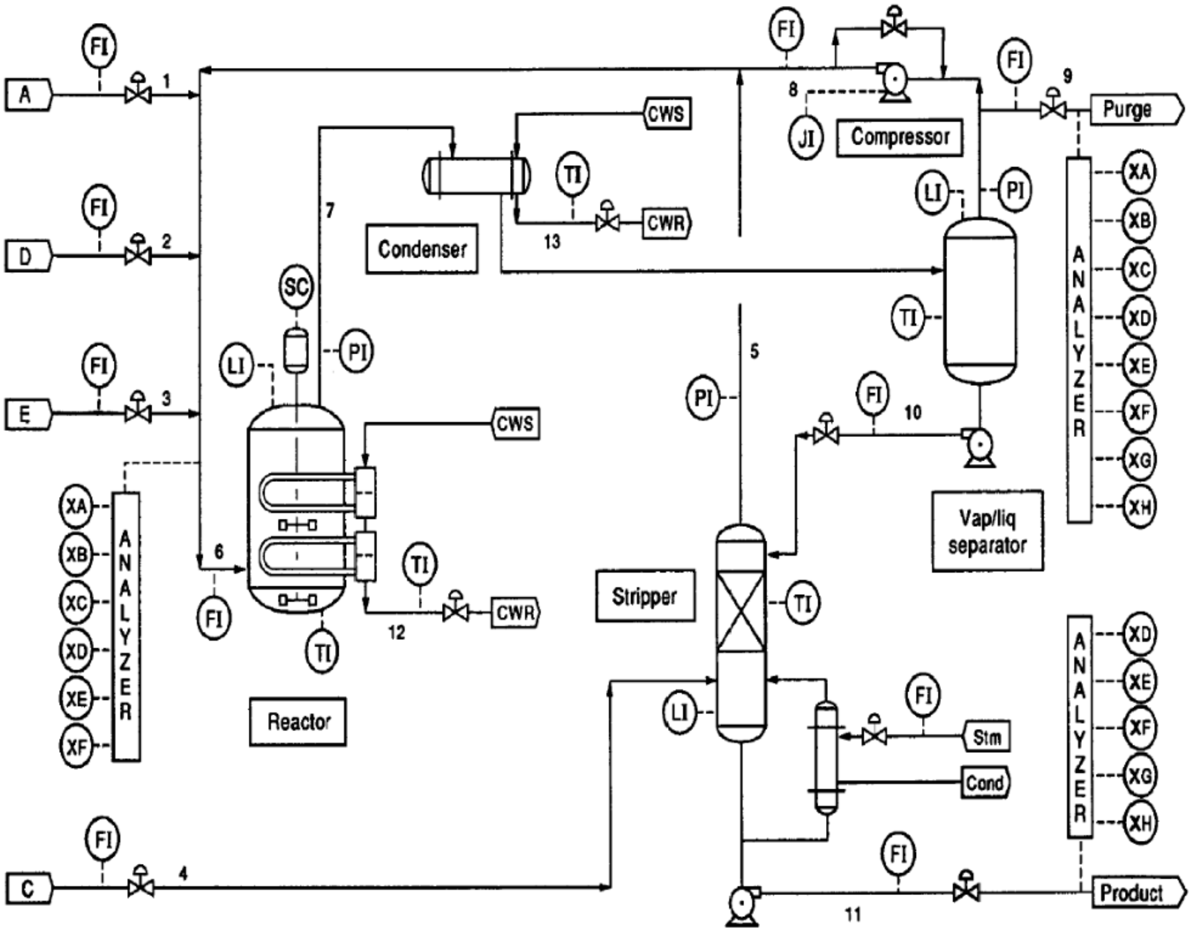


Figure 1. Tennessee Eastman Control Problem (reproduced from [10])

For an analog analysis of performance, a network connection is unnecessary, and instead a channel model may be inserted to simulate the effects of the communication links. The channel model will simulate packet error rates and delay variations of the communications links between sensors/actuators and the controller. Using this approach we will be able to predict in simulation the effect of wireless communication on the performance of the control system.

While a mathematical simulation is an important first step in the analysis of the performance of any system, it will be equally important to understand how a practical system behaves when instrumented with wireless sensing technology that will invariably insert transmission uncertainties. A hardware-in-the-loop (HIL) simulator was therefore constructed to demonstrate the impacts of wireless communication on the performance of the chemical reaction process.

IV. Testbed Implementation

The NIST Industrial Control Systems (ICS) Cybersecurity chemical process testbed presented at the 2014 ISA Process Control and Safety Symposium was adopted as the basis for the wireless testbed [11]. Indeed, the underlying chemical plant simulators are identical. They differ only in the cyber-physical interfaces that are employed for plant performance evaluation. The wireless testbed was constructed using a personal computer (PC)-based simulator, a programmable logic controller (PLC), an IEEE 802.15.4 wireless sensor network, and a Modbus/TCP server. A diagram of the testbed is shown in Figure 2.

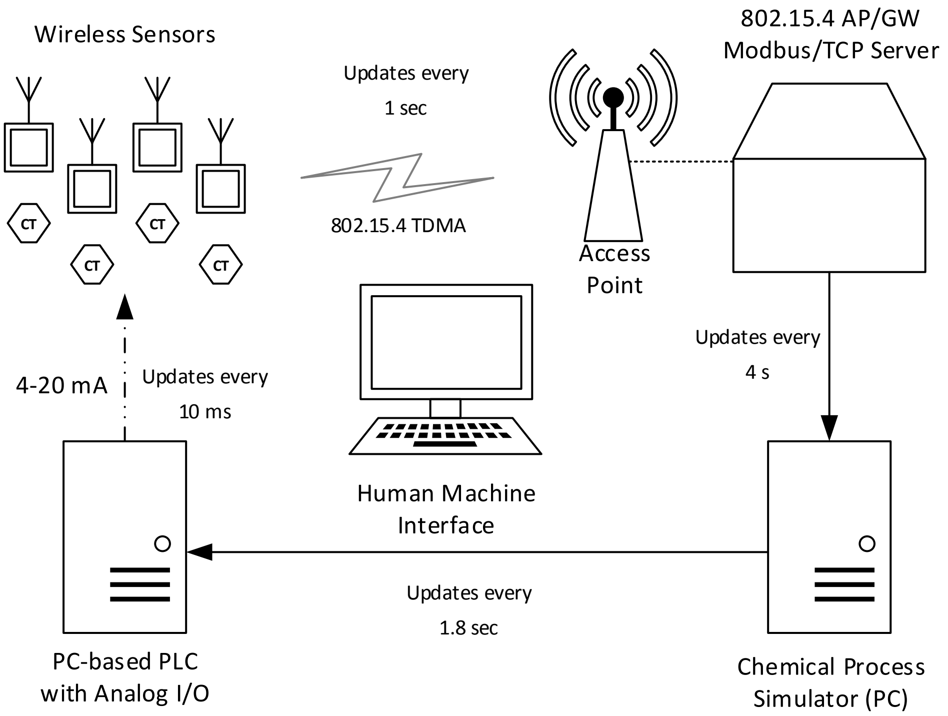


Figure 2. Chemical Process Testbed with Wireless Devices

The chemical plant process is modeled as a first-order system of differential equations as described in [10] and includes the decentralized controller described by Ricker in [12]. The plant and controller processes are herein referred to jointly as the “TE simulator.” The TE simulator is incremented every 0.0005 hour (1.8 seconds). This integration time step was chosen to match the time increment chosen by Ricker for the design of his loop controllers. Modifying the time step may have unintended side effects on the stability of the plant, and therefore was left unchanged.

One of the original requirements for the implementation of the TE simulator as designed by Ricker was simulation speed. However, the TE simulator of our testbed is required to run in real-time, i.e., synchronous to the wall clock. To achieve this goal, a synchronization class (*TETimeSync*) was developed using the *boost::chrono* software module. The simulator is delayed after each increment to slow down the simulation clock enough to match the current wall clock time. If the simulator runs too slowly for real-time, *TETimeSync* detects the condition, and a warning is issued to the console.

A challenge of the testbed was to make the signals compatible with the wireless sensors on-hand. Our wireless sensors are capable of sensing various climatic conditions as well as capable of sensing a 4-20 mA current with varying uncertainty. A PC-based programmable logic controller was used to transfer the TE simulator's current sensor output to the wireless sensor network (WSN) node as shown in Figure 3. A Beckhoff Automation CX2020 PLC with 4-20 mA current output modules was used as the bridging technology. Measured variables (*xmeas*) from the plant process are communicated to the PLC using the Automation Device Specification (ADS) protocol as double precision floating point values. An IEC 61131-3 (Structured Text) program is then used to convert the doubles to signed integers, which are then loaded into the analog output modules. Each wireless node senses the current and transmits the value of the current over-the-air to the wireless gateway where values are stored in a Modbus/TCP server. A Modbus client on the CX2020 polls the Modbus/TCP server for updated current values during each PLC scan and provides the measured variable to the TE Simulator as a floating point value that the TE simulator can use to calculate manipulated values.

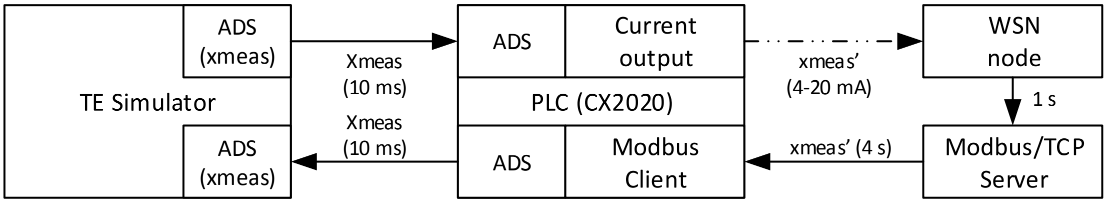


Figure 3. Data Flow of Measured Variables

a) Challenges

Some impact to the performance of the plant process as a result of the wireless network can be attributed to the increase in uncertainty due to sensor calibration errors, network delays, and sensor noises, and the loss of precision of the measured variables resulting from the format conversions. To isolate the effects of these factors from the wireless network, special care was taken to characterize and then minimize those factors.

Sensor Calibration

The first factor affecting plant performance was calibration error of the current sensor within each wireless node. Sensor testing showed an average of 1.4 mA offset for each sensor across all current input levels as show in Figure 4. In addition, the calibration offset drifted with time by +/- 0.1 mA. For the purpose of measurements, the average offset was corrected after the reading was pulled from the Modbus/TCP server.

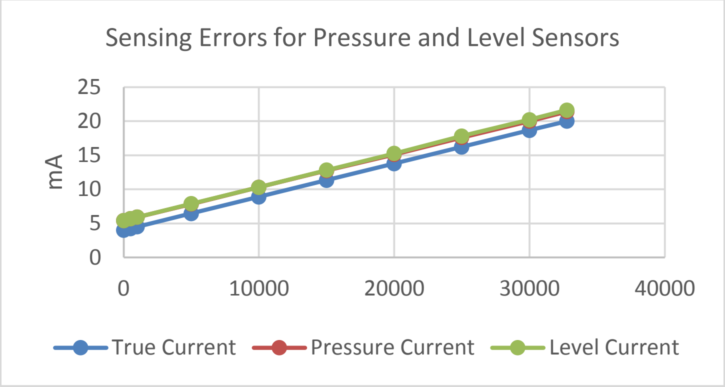


Figure 4. Current Sensing Errors

Real-time Time Correlation

Another challenge to integrating a PC-based simulation of the TE chemical process with wireless sensors was maintaining real-time correlation between the observable states of the simulated chemical process variables with the representative current outputs from the PLC. This problem was solved by configuring the PLC scan time to 10 ms, which is sufficiently faster than the integration time step of 1.8 s within the PLC. The PLC adjusts the current within 10 ms, which is much faster than the signal update rate from the TE simulator.

Configurability of the Wireless Sensor Network Components

Typical wireless sensor networks provide sufficient configurability by providing the operator with a fine-tuning capability of the acquisition rates, wireless sensor transmission rates, and automation server storage update rates. Our wireless sensor network did not provide a high degree of configurability in all cases. One area of concern in our system was the Modbus/TCP server update rate. Our system allowed for the transmission of sensor values from the various nodes every second; however, the gateway updates the Modbus database only every 4 seconds, thus dropping the intermediate readings. This is conformant with the required burst rate for WirelessHART sensor devices, and this is compatible with the requirements of the TE simulator.

Assuming an ideal RF communication channel, the Primary remain disturbance due to the network can be calculated based on known delay constants. The worst case per reading delay from signal acquisition to actuation was determined to be 5.02 s.

V. Test Scenarios

As indicated by Ricker, most control theory analyses focus on metrics of loop controllers with little attention given to areas of control that plant operators consider. In an attempt to address both technical factors and operational factors, scenarios were carefully chosen to match the set-points and disturbances addressed by Ricker in [12]. These process control scenarios are listed in Table 1. For each experimental scenario, a baseline scenario was run without the wireless sensor network to represent the ideal case, such as lossless, noise-free, latency-free conductors similar to that of classical copper wire control loops. Therefore, each scenario produced a baseline data set and an experiment data set.

Table 1. Experimental Scenarios for Wireless Sensing and Control Analysis

Scenario	**Description**
Reactor Level	The level set-point of the reactor is modified to 80.1% from 65 %
Reactor Pressure	Reactor pressure set-point adjusted downward to 2700 kPa from 2800 kPa.
Production Rate	Production rate set-point is modified to 25 from 22.89
Quality Factor	% mol. G set-point is modified to 35 % from 53.8 %
Stuck Reactor Cooling Valve	The valve controlling cool water flow to the reactor does not respond to commands.

VI. Results

The chemical process wireless testbed was exercised with the scenarios listed in Table 1. For each scenario, the measured variables as reported by the TE simulator were collected every 20 integration time steps of the simulator. Values were stored in a tabbed delimited file for offline processing. Metrics were then collected for each scenario to include statistical quantities, such as mean, median, quantiles, and outliers of each measured variable as well as the difference of the measured variable to its baseline. Deviations were measured as the percentage difference of the experimental case to the baseline case for each signal. In addition, plots of the time series for baseline and experimental cases were qualitatively compared attempting to explain the differences in statistical results.

Example statistical measures are listed in Table 2 and a graphical representation of the distribution of deviations from baseline is provided in Figure 5. This particular scenario shows the experimental deviation when the reactor pressure set-point was lowered from 2800 kPa to 2700 kPa. The figure shows that when changing the set-point using a wireless network versus a faster, and presumably more reliable, wired network, most measured variables tracked the baseline case closely. While the costs for operating the plant showed significant deviations with periods of higher costs of more than 100 %, closer examination of the time series (Figure 6) showed that deviations were due to a lag in the time series response.

By referring to Figure 6, we may also be able to explain this discrepancy by the longer settle times and larger overshoots of the key process variables for a small period of time between 3 and 4 hours. We have observed large deviations in inventories (i.e., tank levels) during this time, which could lead to larger hourly costs. Eventually, the experimental case settles to track the baseline case, and it is conceivable that optimization algorithms could be used to minimize these deviations. Calculation of the cost function is defined in "MultiLoop_mode1.mdl" in the *Tennessee Eastman Challenge Archive* [14].

Table 2. Statistical Summary of the % Difference from Baseline for the Reactor Pressure Change Scenario

Variable	*Min*	*Max*	*Mean*	*Std. Dev.*
Reactor.Pressure.kPa	-1.3	1.30	-0.02637	0.27
Reactor.Level.Pct	-5.5	22.90	-0.05048	1.76
Reactor.Temp.C	-0.3	0.05	0.00009	0.01
Sep.Level.Pct	-16.6	31.34	-0.06063	7.24
Stripper.Level.Pct	-20.9	78.42	2.13762	21.19
Sep.Underflow.m3.hr	-3.7	6.31	-0.36017	1.56
React.Cool.Temp.C	-0.1	1.12	0.00142	0.15
Product.G.mole.Pct	-1.1	0.53	0.00329	0.26
Hourly.Cost	-38.5	134.78	3.79610	20.08

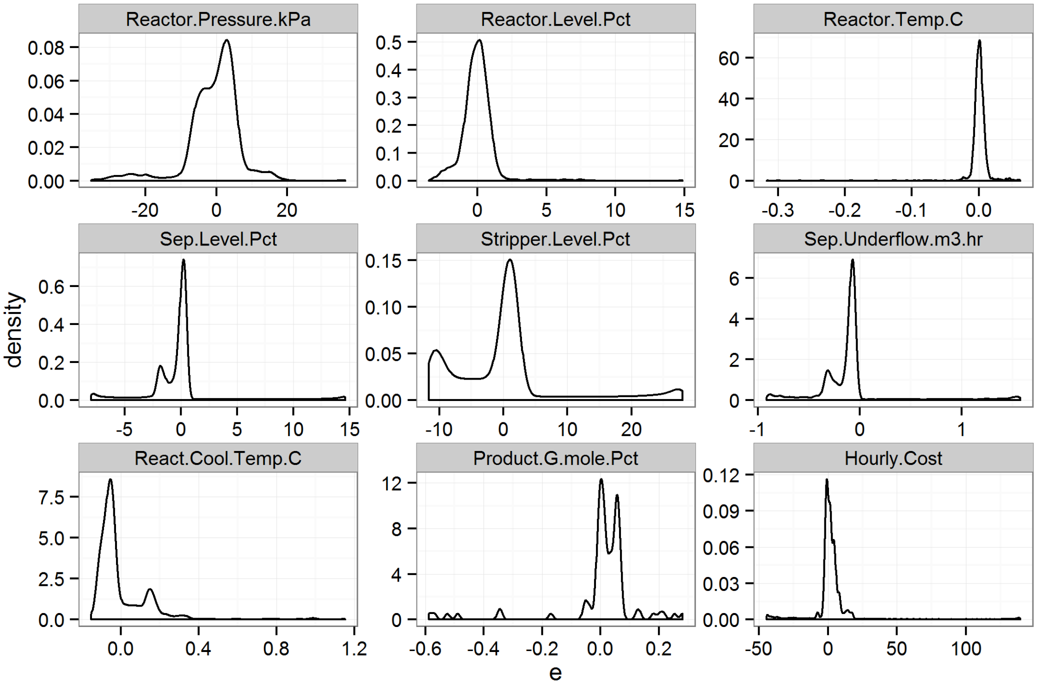


Figure 5. Probability Distribution of Percent Deviation (e) for a Change in Reactor Pressure to 2700 kPa. The horizontal axis is the percent error, and the vertical axis is the probability of deviation.

Another scenario considered was disturbance rejection for which a stuck valve condition was created. In this scenario, the valve controlling the flow of cold water to the reactor was rendered "stuck" in the closed position. The figure shows that when the cooling valve malfunctions, the wireless network impacts the performance of all process variables especially stripper inventories. In this case, an update rate limitation of the Modbus/TCP server within the wireless gateway could be considered a root cause for deviations reported by the plant simulator; however, this would be a legitimate concern for network control integrators and indicates the need for careful study of all system components prior to a wireless network deployment.

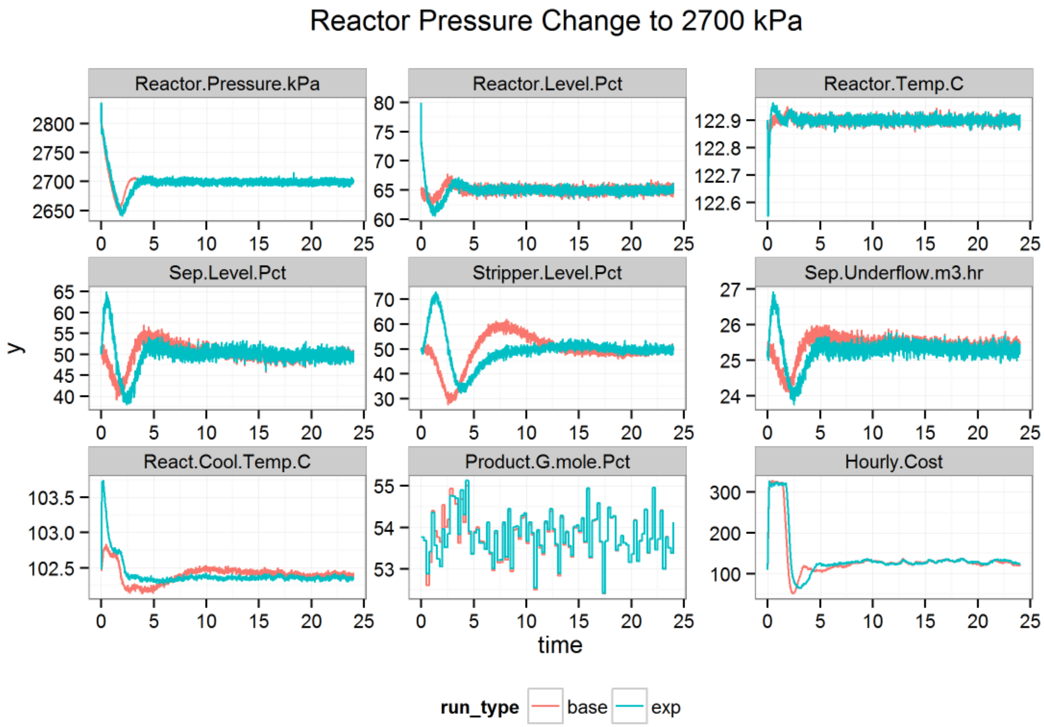


Figure 6. Time Series Evaluation for Change in Reactor Pressure.
Legend: *base*=wired/ideal, and *exp*=wireless

Table 3. Summary of % Difference from Baseline for Stuck Valve Scenario

Variable	*Min*	*Max*	*Mean*	*Std. Dev.*
Reactor.Pressure.kPa	-0.7	1.0	-0.00399	0.2
Reactor.Level.Pct	-5.2	13.1	-0.05651	1.6
Reactor.Temp.C	-0.5	0.5	0.00003	0.2
Sep.Level.Pct	-11.1	28.8	-0.23135	6.6
Stripper.Level.Pct	-33.9	55.5	0.46037	19.9
Sep.Underflow.m3.hr	-2.7	6.0	-0.45053	1.5
React.Cool.Temp.C	-1.2	1.5	0.01762	0.5
Product.G.mole.Pct	-1.1	0.5	-0.01470	0.3
Hourly.Cost	-37.1	22.9	-1.56317	10.4

VII. Future Work

The work presented here provides a workable prototype for the development of well-thought scenarios for studying wireless networks used by the process control industry. As a prototype, areas of improvement are necessary for the development of more accurate test scenarios that reflect the real world process control environments. Future iterations of the testbed will include the following elements:

- RF channel emulation. A channel emulator provides a means to recreate the RF environment in a laboratory setting. Conditions, such as interference, propagation effects, and jamming can be applied to RF signals and the effects on the physical process may be studied.
- Calibration: While steps were taken to overcome calibration error uncertainty, better current sensing circuits should be added to minimize the possibility that sensing error contributes to deviations from baseline more than the network.
- Actuators: The current implementation of the testbed does not allow for closed-loop control over wireless. An objective of the testbed is to evaluate the impacts of closed-loop control over wireless networks; therefore, wireless actuators will be added to the testbed as they are made available.
- Timestamps: Timestamp allows for improved signal processing, such as interpolation and extrapolation. Timestamping is not available with the current Modbus/TCP interface to the controller. Using another industrial interface would allow for more advanced signal processing, such as predictive filtering and model-based control.

VIII. Conclusions

A testbed for the study of chemical process control was constructed for the purpose of studying the effects of wireless network performance on the control of physical processes. The Tennessee Eastman chemical reactor process was chosen as a genuine example of a real-world manufacturing process using a model that has been widely accepted by researchers and practicing engineers. The testbed implements a hardware-in-the-loop architecture by incorporating a simulation of the plant process and decentralized controller with an IEEE 802.15.4 TDMA-based wireless sensor network for measured variables and a wired factory automation network for manipulated variables. In addition, the testbed provides the ability to recreate the RF environment unique to any factory and measure the performance impacts of the RF environment on both the wireless network as well as the performance of the physical process. Time series data of measured process variables and performance metrics of the physical process were collected to demonstrate the impact of a wireless sensing network on factory performance. Preliminary results were collected without the RF emulation capability in place. These results demonstrate the capability of the testbed to generate and collect plant-centric sensor data for process control and performance evaluation. Future data will include RF channel emulation of the plant environments.

Acknowledgments

We would like to thank Rushad Antia and Luke Roepe for their contributions in software development in support of the experimentation.

Source Code

All software code for the TE simulator may be found at the *tesim* GitHub repository by visiting http://www.github.com/usnistgov/tesim. Researchers are encouraged to reuse the software for their own investigations.

Disclaimer

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

References

[1] World Economic Forum, “Industrial Internet of Things : Unleashing the Potential of Connected Products and Services,” Cologny/Geneva , Switzerland, 2015.

[2] “Industrial WSN Report 2014,” ON World, San Diego, CA, 2014.

[3] T. Moore, “Research: Wireless use in industry,” *Control Engineering Magazine*, 2013. [Online]. Available: http://www.controleng.com/single-article/research-wireless-use-in-industry/5b97f5d429813c649a05240ad5efd280.html.

[4] W. J. Miller, “Wireless Takes Control,” *International Cement Review*, p. 88, 2008.

[5] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, “Comparison of Industrial WSN Standards,” pp. 632–637, 2010.

[6] D. Chen, M. Nixon, and A. Mok, *WirelessHART^{TM}*. Boston, MA: Springer US, 2010.

[7] “ZigBee Wiki Article.” [Online]. Available: https://en.wikipedia.org/wiki/ZigBee.

[8] G. Wang, “Comparison and Evaluation of Industrial Wireless Sensor Network Standards ISA100 . 11a and Wireless HART Master of Science Thesis , Communication Engineering,” Gothenburg, Sweden, 2011.

[9] C. Alcaraz and J. Lopez, “A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems,” *IEEE Trans. Syst. Man, Cybern. Part C (Applications Rev.*, vol. 40, no. 4, pp. 419–428, 2010.

[10] J. J. Downs and E. F. Vogel, “A Plant-wide Industrial Problem Process,” *Comput. Chem. Eng.*, vol. 17, no. 3, pp. 245–255, 1993.

[11] R. Candell, K. Stouffer, and D. Anand, “A Cybersecurity Testbed for Industrial Control Systems,” in *Proceedings of the 2014 Process Control and Safety Symposium*, 2014.

[12] L. Ricker, “Decentralized control of the Tennessee Eastman Challenge Process,” *J. Process Control*, vol. 6, no. 4, pp. 205–221, Aug. 1996.

[13] M. M. Krotofil and D. Gollmann, “Industrial control systems security: What is happening?,” in *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, 2013, pp. 670–675.

[14] L. Ricker, “Tennessee Eastman Challenge Archive.” [Online]. Available: http://depts.washington.edu/control/LARRY/TE/download.html.

Analysis of Virtual Networking Options for Securing Virtual Machines

Ramaswamy Chandramouli
Computer Security Division, Information Technology Laboratory
National Institute of Standards & Technology
100 Bureau Drive, Gaithersburg, MD, USA
E-Mail: mouli@nist.gov

***Abstract* – Virtual Machines (VMs) constitute the primary category of resources to be protected in virtualized infrastructures. Out of the two types of protection for VMs – Host-level and Network-level – it is the approaches for the Network-level protection that are different in virtualized infrastructures as compared to those for non-virtualized environments. This is due to the fact that the VMs are end nodes of a virtual network as opposed to being end nodes of a physical network. In this paper, we provide a detailed analysis (in terms of advantages and disadvantages) of some of the key approaches for two Network-level protection measures for virtualized infrastructures – Network Segmentation and Traffic Control using Firewalls. The choice of these two Network-level protection measures is due to the fact that they form the foundation for the network configuration of the entire virtualized infrastructure. We also provide the overall conclusions from the analysis in the form of recommended deployment choices based on approaches for these two network-level protection measures for securing VMs.**

Keywords - Virtual Machine; VLAN; Hypervisor; VXLAN; Virtual Firewall.

I. INTRODUCTION

Virtualized hosts (also called hypervisor hosts) are increasingly deployed in data centers because of efficiency, scalability and cost considerations. The virtualized infrastructure resulting from the deployment of virtualized hosts has three main categories of components - Hypervisor Software, Virtual Machines (VMs) and Virtual Networking components such as Virtual Network Interface Cards (vNICs), Virtual Switches and Virtual Firewalls.

Out of the three categories of components above, the VMs constitute the fundamental resource to be protected in a virtualized infrastructure, since they are the compute engines on which business/mission critical applications of the enterprise run. These VMs are virtual counterparts of physical servers and hence just like their physical counterparts, security for these VMs has to be provided through host-level and network-level measures. These measures may also vary depending upon whether the overall virtualized infrastructure (in which the VM resides) is used for in-house enterprise applications or for offering cloud services to external entities (e.g., Infrastructure as a Service Public Cloud). We provide a brief overview of the two types of protection mentioned above. (a) Host-level protections required for VMs include features for robust authentication, access using secure access protocols and secure session establishment. The mechanisms required for providing these features are no different for VMs compared to their physical counterparts (i.e., physical servers). (b) Network-level protections required for VMs are feature-wise similar to those that are required by their physical counterparts. However, the mechanisms or approaches required for providing these protections are different due to the fact that the VMs are end nodes of a virtual network as opposed to being end nodes of a physical network.

For any type of datacenter infrastructure (virtualized or non-virtualized), there is a general consensus that the following are some of the key Network-level protection measures [1]. They are: (a) Network segmentation or isolation, (b) Traffic control using firewalls, (c) Creating Redundant communication pathways, and (d) Traffic Monitoring and Prevention using IDS/IPS.

Out of the above four network-level protection measures, the first two - Network Segmentation and Traffic Control using Firewalls - form the foundation for the network configuration of the entire virtualized infrastructure. Hence, in this paper, we have chosen to focus on different approaches or mechanisms used for these two network-level protection measures, by performing a detailed analysis of the advantages and disadvantages of each of the approaches.

Copyright (c) The Government of USA, 2016. Used by permission to IARIA. ISBN: 978-1-61208-460-2

Before we describe the organization of the rest of the paper, a few observations regarding our chosen network-level protection measures in the context of virtualized infrastructure are in order. In a virtualized infrastructure, the distinguishing networking environment is the virtual network. Hence the network segmentation approaches discussed in this paper have to involve some virtual network components such as virtual switches. Similarly, a viable approach for traffic control using firewalls has to use a virtual firewall instead of a physical firewall. In Section II, we focus on two network segmentation approaches and discuss the advantages and disadvantages of each. Control of virtual network traffic using two different types of virtual firewalls and the advantages and disadvantages of each are analyzed in Section III. In Section IV, we provide the overall conclusions from the analysis, in the form of deployment choices based on approaches for the two network-level protection measures for securing VMs.

II. NETWORK SEGMENTATION IN VIRTUAL NETWORKS

The approaches to network segmentation in the context of virtualized infrastructures are the same as those used in physical network with some variations (these variations are underlined in our description below): (a) Using a combination of firewalls – the firewalls used are virtual firewalls (as opposed to a physical firewall) and are implemented as Virtual Security Appliance (VSA) and hosted on security hardened VMs with multiple Virtual Network Interface cards (vNICs). Each vNIC may be connected to a different network segment [2]. (b) Isolated network segments created as logical segments on top of a physical network segment – one is the VLAN approach that is based on tagging packets and switch ports with a unique identifier called VLAN ID, and the other is overlay-based virtual networking technology that creates an overlay network by encapsulating packets with IDs depending upon the type of overlay technology. Both approaches (VLAN and Overlay) rely on the capabilities in virtual switches of the virtualized host.

The three approaches for network segmentation in virtualized infrastructures outlined above are discussed in Sections A, B and C below. After a brief description of each approach, an analysis of each approach is provided with the relative advantages and disadvantages. Where ever applicable, the distinct advantage of a particular approach is also brought out.

A. Network Segmentation Using a Combination of Firewalls

Let us now consider a virtualized host with 4 VMs – VM1, VM2, VM3 & VM4. We can form a network segment (say a DMZ) using two virtual firewalls, one each on any two VMs - say VM1 & VM4. These firewalls are VM-based Virtual Security Appliances residing on VMs defined with multiple vNICs – each one connected to a different network segment. The firewall in VM1 then will have one vNIC connected to an external network (say the public Internet) of the enterprise and the other vNIC connected to the DMZ segment in the virtualized network within a virtualized host. Correspondingly the firewall in VM4 has to have one vNIC connected to the internal network of the enterprise and the other vNIC connected to the DMZ. The vNIC connection to the DMZ (from both firewall VMs - VM1 & VM4) is established by their pathway to an internal-only virtual switch. This internal-only virtual switch has no uplink connection to any physical NIC of the virtualized host and hence traffic from any VM connected to it cannot travel directly outside the virtual network segment (not to speak of outside the virtualized host). The internal-only switch can only forward traffic directly to VMs connected to it - say VM2 &, VM3. All incoming and outgoing traffic into the VMs connected to the internal-only virtual switch whose source/target is an internal/external network, has to go through the firewall in VM1 or in VM4. The firewalls in VM1 & VM4 thus form the gatekeepers for the virtual network segment (i.e., DMZ).

A.1 Analysis

The advantages of network segmentation within the virtualized network of a virtualized host using a combination of virtual firewalls are: (a) Simplicity of Configuration: It can be configured with commodity firewall VSAs hosted on multi-vNIC VMs. (b) Flexibility within a Virtualized host: More than one isolated network segment can be created within the virtual network of the virtualized host by simply adding another firewall VM.

The limitations of this approach to network segmentation in a virtualized network are the following: (a) The logical network segment created inside a virtualized host can neither be extended to the physical network of the data center nor to the virtual network in another virtualized host (since segmentation is obtained by virtual firewalls inside the virtualized host). This makes the approach to network segmentation non-scalable. (b) A consequence of creating a non-scalable network segment is that the migration of a VM in the network segment to any other virtualized host (due to

SP-155

Copyright (c) The Government of USA, 2016. Used by permission to IARIA. ISBN: 978-1-61208-460-2

performance or availability or load balancing reasons) is out of the question, unless a network segment (with identical configuration) exists on the target virtualized host.

B. Network Segmentation Using Virtual LAN (VLAN) Technology

The second approach to network segmentation in virtualized infrastructures is broadcast-containment networking technologies, such as VLAN. The requirement for this is that the hypervisor should have capabilities to define virtual switches that are VLAN-aware [3][4]. The segmentation is obtained by assignment of an identifier called the VLAN ID to one or more ports of a switch and connecting the VMs designated for that VLAN segment to those ports. VMs on one VLAN can only communicate directly with VMs on the same VLAN and a router is needed for communication between VMs on different VLANs [5]. Assignment of a VM to a particular VLAN can be based on the application tier it is hosting (e.g., Web Server, DBMS server, etc.) or the client to which the VM belongs (in cloud data centers). These VLAN-capable virtual switches (VS) can perform tagging of all packets going out of a VM with a VLAN tag (depending upon which port it has received the packet from) and can route an incoming packet with a specific VLAN tag and MAC address to the appropriate VM by sending it through a port whose VLAN ID assignment equals the VLAN tag of the packet. An example of a VLAN-based virtual network segmentation inside a virtualized host is given in Figure 1.

B.1 Analysis

The advantages of a VLAN-based network segmentation approach are: (a) Network segments can extend beyond a single virtualized host (unlike the segment defined using virtual firewalls) since the same VLAN ID can be assigned to ports of virtual switches in different virtualized hosts. (b) The number of network segments that can be configured is reasonably large since a single virtual switch can typically support 64 ports and the 12-bit VLAN ID address space enables creation of 4000 VLAN segments.

The disadvantages of VLAN-based network segmentation approach are: (a) The configuration of the ports in the physical switch attached to a virtualized host must exactly match the VLANs defined on the virtual switches inside that virtualized hosts. This results in tight coupling between virtual network and physical network of the data center. The consequence of this tight coupling is that the port configuration of the physical switches has to be frequently updated since the VLAN configuration of the virtual network of the attached virtualized host may frequently change due to migration of VMs among VLANs as well as among virtualized hosts. (b) Another consequence of frequent migration of VMs among VLANs, as well as among virtualized hosts is that the VLAN configuration of ports in the physical switch may not match with that of the connected virtualized host. This may result in a situation where a particular hypervisor (or a virtualized host) may end up processing messages for every VLAN on the network, even when it is not hosting any active VM belonging to that VLAN [6] and (c) Segments created using broadcast-containment technologies cannot be allowed to have a large span since they will result in greater traffic in the overall data center due to multicast and broadcast traffic. But greater VM mobility (due to load balancing and availability reasons) may require VLANs with a large span resulting in an undesirable phenomena called VLAN sprawl [6].

C. Network Segmentation Using Overlay-based Virtual Networking Technology

In the VLAN-based approach, the logical network segments were created on a physical LAN using portgroups of virtual switches inside virtualized hosts. These logical network segments did span multiple virtualized hosts. The total number of these segments possible is limited to around 4000 due to the 12 bit address space of VLAN ID. Another limitation is the lack of independence between the physical and virtual networking infrastructure, since the port configuration of the physical switches attached to the virtualized hosts have to be consistent with the VLANs defined on the port groups of virtual switches inside those virtualized hosts. The overlay-based virtual networking approach to network segmentation overcomes these two limitations in the following two ways [7].

Copyright (c) The Government of USA, 2016. Used by permission to IARIA. ISBN: 978-1-61208-460-2

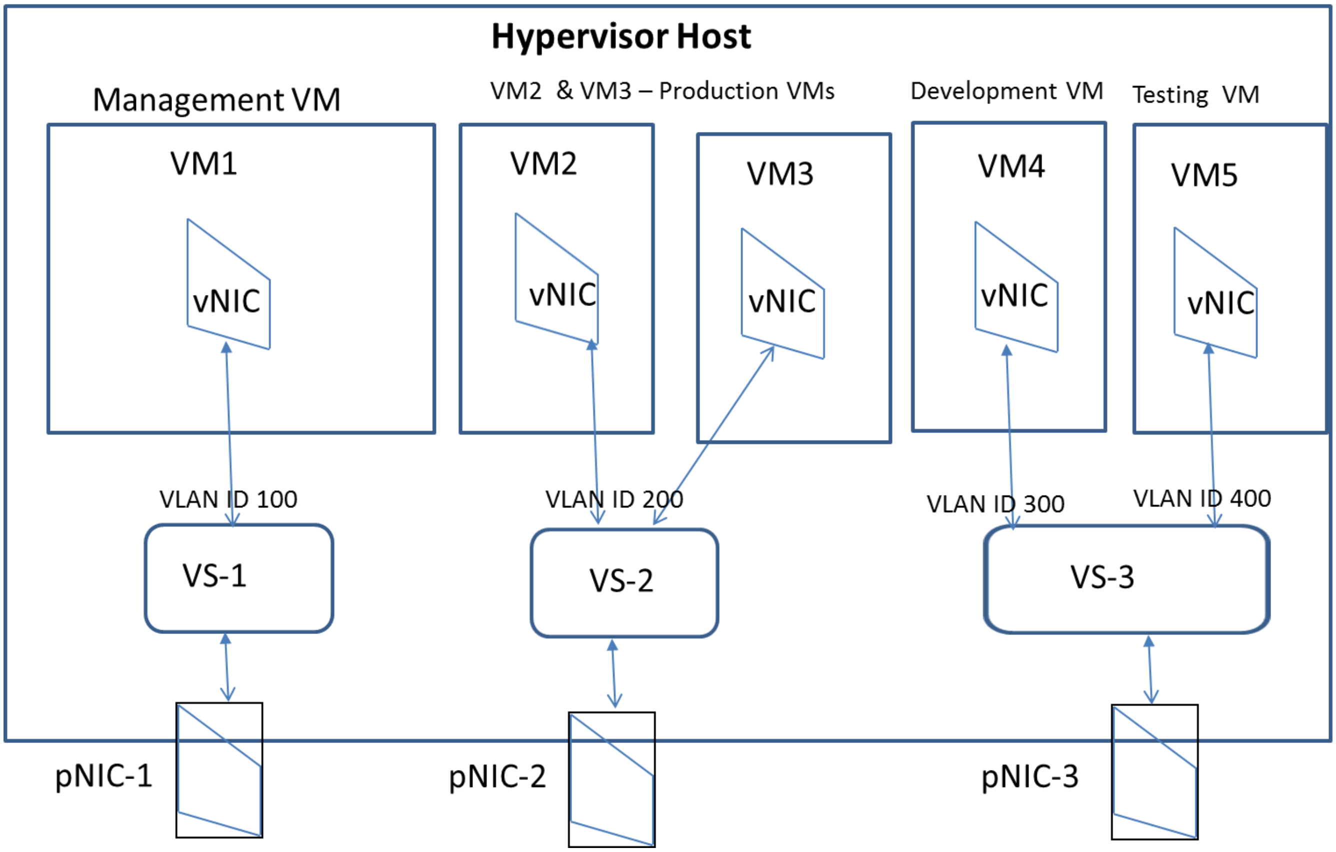


Figure 1 - VLAN-based Network Segmentation

(a) Overlay-based virtual networking technologies have a larger address space enabling larger number of virtual network segments. An example is the 24 bit VXLAN ID of the VXLAN overlay scheme that can enable 16 million virtual network segments to be defined, and (b) The overlay schemes by their definition, create a logical Layer 2 network (called the overlay network) over the physical Layer 3 backbone of the data center (called the underlay network). Since this scheme does not warrant any modifications to the physical network, it provides physical-logical network independence. As already alluded to, overlay-based virtual networking schemes achieve segmentation by creating a logical Layer 2 network over the physical Layer 3 network. The overlay network is created by encapsulating a native Layer 2 packet with another Layer 2 identifier. There are three common encapsulation schemes – VXLAN, GRE and STT [8].

Let us now look at the encapsulation process in VXLAN [9] through components shown in Figure 2. The Ethernet frame originating from a VM, that just holds the MAC address of the destination VM is encapsulated in two stages: (a) First with the 24 bit VXLAN ID (virtual Layer 2 (L2) segment) to which the sending/receiving VM belongs and (b) Second, with the source/destination IP address of the VXLAN tunnel endpoints called VTEPs. [10]. VTEPs are logical network endpoints (nodes) for the encapsulated VXLAN packets and they reside in the kernel of a hypervisor. A VXLAN-encapsulated packet originates at the VTEP in the kernel of the hypervisor where the source VM resides (carrying the VTEP's address as the source IP address) and terminates at the VTEP in the kernel of the hypervisor where the destination VM resides (carrying this VTEP's address as the destination IP address). Thus, we see that VXLAN encapsulation enables creation of a virtual Layer 2 segment that can span not only different hypervisor hosts but also different IP subnets within the data center.

C.1 Analysis

The advantages of a network segmentation approach based on Overlay-based networking technology are: (a)

Copyright (c) The Government of USA, 2016. Used by permission to IARIA. ISBN: 978-1-61208-460-2

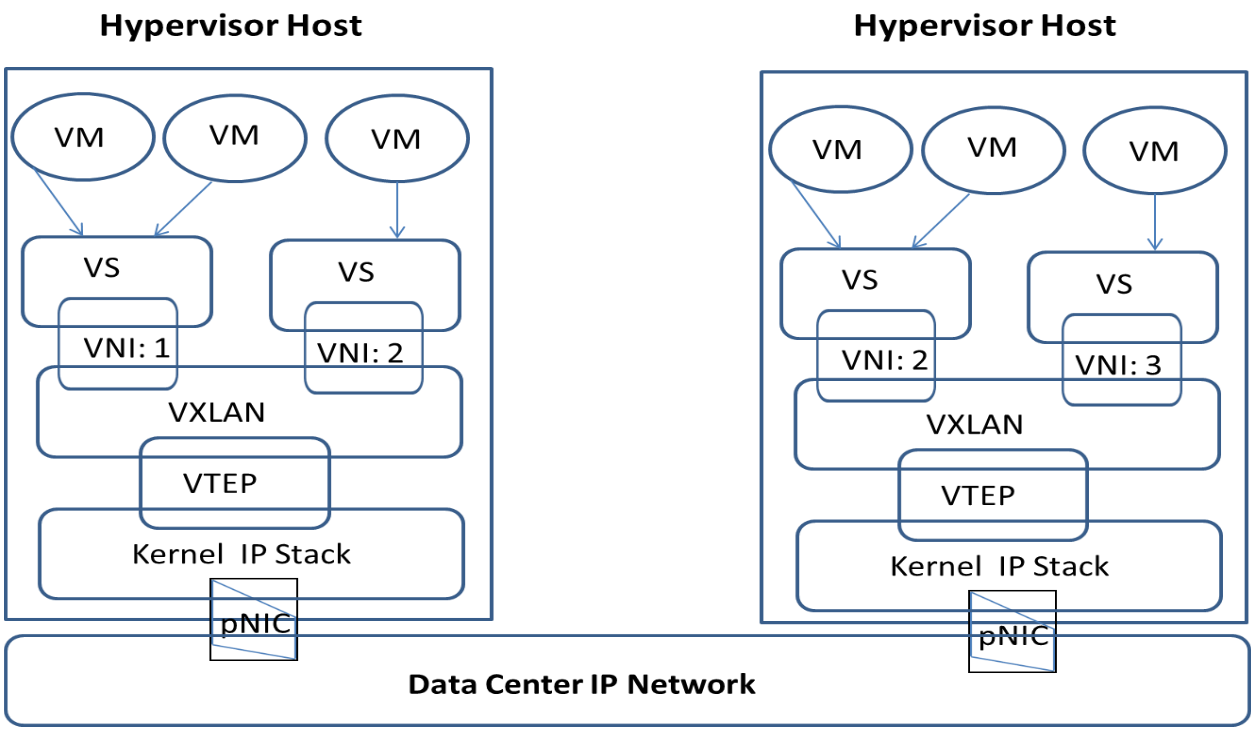


Figure 2 – Overlay-based Virtual Network Segmentation

Because of independence between the virtual network and the physical network, there is greater VM mobility compared to a VLAN- based virtual network environment, (b) The physical-logical network independence, together with the bigger overlay segment ID address space (e.g., a VXLAN ID is 24 bits as opposed to 12 bit VLAN ID allowing for 16 million segments compared to 4096 for VLAN), makes the overlay based network segmentation infinitely scalable. Another factor contributing to scalability of the overlay scheme is that the encapsulating frame is an IP/UDP packet. Hence, the number of virtual network segments is limited only by the size of IP subnets that can be defined within the data center and not by the number of ports in virtual switches as in the case of VLAN-based network segmentation. Further, by using internal, non-routable IP addresses for VMs (using DHCP and NAT capabilities) running within virtualized hosts, the number of virtual networks that can be realized is even higher and (c) The VLAN scheme uses the Spanning Tree Routing Protocol to forward packets, VXLANs can use the ECMP protocol of Layer 3 [11], thus efficiently utilizing all available network links in the network fabric of the data center.

The disadvantage of a network segmentation approach based on Overlay-based networking technology is that it requires large mapping tables in each virtual switch level in order to generate overlay packets – since the MAC address of the destination VM could be located in any IP subnet and any host in the data center. Building these mapping tables using just a flooding technique is inefficient. Hence, a control plane needs to be deployed in the virtualized infrastructure to populate the mapping tables for use by the overlay packet generation module in the hypervisor. This creates an additional layer of control and adds to the complexity of network management [11].

III. TRAFFIC CONTROL IN A VIRTUAL NETWORK

Traffic control in a virtual network can be performed using either a virtual firewall or a physical firewall. However, in a virtualized infrastructure, the computing nodes (whose incoming/outgoing traffic needs to be controlled) are VMs and are end nodes of a virtual network. Hence, the deployment of a physical firewall will require the traffic from the virtual network to be diverted into the physical network (where the physical firewall resides) and

Copyright (c) The Government of USA, 2016. Used by permission to IARIA. ISBN: 978-1-61208-460-2

then back into the virtual network. This extra route travelled by communication packets will result in latency and consequently reduced performance of applications hosted on VMs. Hence, in this paper, we consider only virtual firewall-based solutions for traffic control in virtual networks for securing VMs.

Earlier in this paper (Section 2), we saw that two or more virtual firewalls can be used to create network segments in a virtual network. Since the focus of this Section is on traffic control, we are going to analyze the use of virtual firewalls only for controlling inter-VM traffic.

Inter-VM traffic can be of two kinds: the traffic between two VMs residing on the same virtualized host (either connected to the same or different virtual switches) and traffic between two VMs hosted on different virtualized hosts. Traffic between two VMs residing on the same virtualized host can only be enabled if each VM has at least one vNIC (a VM can have multiple vNICs just like a physical server can have multiple physical network interface cards or network adapters) connected to a common virtual switch. This is due to the fact that two virtual switches in a virtualized host cannot be connected to each other. Although, theoretically, a pathway between two VMs on the same virtualized host can be establishing by routing the traffic from one VM (say VM1) to the physical network (through one physical NIC) and back into the same virtualized host (through another physical NIC) to the target VM (say VM2), this is not a viable option in most situations, due to the latency issue referred to above. Of course, for enabling traffic between two VMs residing on two different virtualized hosts, the traffic has to travel from the virtual network (in the originating virtualized host) where the originating VM resides, through the physical network of the data center and back again into the virtual network of the target VM (in the target virtualized host).

Virtual firewalls come in two flavors: (a) VM-based – this class of virtual firewalls, comes packaged as a virtual security appliance on a specially-configured VM and (b) Hypervisor Kernel-based – this class of firewalls operates as a kernel loadable module in the kernel of the hypervisor.

A. Traffic Control using VM-based Firewalls

A VM-based firewall, as the name indicates, is a firewall software that runs in a VM. It can be installed as a software module on a guest VM already running in a virtualized host or it can be packaged as a virtual security appliance on a specially prepared VM instance. Its location within the virtual network of a virtualized host is critical as its function is to monitor, drop or forward packets between sets of VMs belonging to different security zones. This is the reason that this class of firewalls is called bridge-mode firewalls as it also acts as a bridge between zones (since the only link between VMs connected to two different virtual switches is through a VM with vNICs connected to both virtual switches).

A.1 Analysis

The advantage of VM-based firewall for traffic control is that since it is available as a Virtual Security Appliance, it is easy to deploy and configure in a virtualized host. Its initial location within the virtual network of the virtualized host is relatively easy as it is dictated by the layout of the security zones based on the various virtual switches and this type of firewall only monitors and filters packet flows between one virtual switch and another.

The disadvantages of VM-based firewalls are: (a) It cannot monitor and filter traffic flowing between two VMs connected to the same virtual switch, (b) Its performance is limited by the number of virtual CPU cores allocated to the VM it is residing or packaged in, and (c) All traffic flowing into and out of all portgroups and virtual switches associated with zones pertaining to this firewall, has to be redirected to this firewall causing unnecessary traffic (a phenomena called Traffic Trambones [12]).

B. Traffic Control using Hypervisor Kernel-based Firewalls

Hypervisor kernel-based firewalls are also called hypervisor-mode firewalls and VM NIC firewalls. These firewalls install as a hypervisor module along with a VSA, the latter used purely for initial configuration (and re-configuration) for the hypervisor module. Hence, the main firewall functions of monitoring and packet filtering are done in the hypervisor kernel-module with the VM hosting the VSA portion playing the role of a Control or Service VM. Logically residing between a VM vNIC and the hypervisor virtual switch, this type of firewall provides a vNIC-level firewall enforcement point for traffic to and from VMs. Thus they can be used for selectively protecting a given subset or all the VMs in a host or a cluster. Because of the visibility at the vNIC level, these firewalls can protect traffic flowing between two VMs connected to the same virtual switch, unlike the bridge-mode firewalls. Another distinguishing feature of this type of firewalls is that the firewall does not require any changes

Copyright (c) The Government of USA, 2016. Used by permission to IARIA. ISBN: 978-1-61208-460-2

to the virtual network configuration inside a virtualized host (such as additional network pathways for redirecting traffic to the VM hosting firewall) or modification to IP addresses of VMs.

B.1 Analysis

The advantages of hypervisor kernel-based firewalls are: (a) Their performance is of an order of magnitude much higher than bridge-mode firewalls since they perform packet inspection from within the kernel at native hardware speeds rather in a VM where the performance is limited by the capacity of virtual CPU allocated to it [13], (b) These perform monitoring at the VM NIC (vNIC) level and hence all firewall rules (or ACLs) and state are logically attached to the VM interface. Hence these rules and state move with the VM when it migrates from one virtualized host to another, thus providing continuity of security protection for a VM irrespective of its location [12], and (c) Implementations that support firewall rules at a higher level of abstraction than IP addresses or ports, can be used to filter packets at data center, host cluster and port group levels.

The disadvantages of hypervisor kernel-based firewalls are: (a) This class of firewalls works as a managed kernel process and is therefore neither a VM resident program nor is part of the virtual network of the hypervisor. Hence conventional management tools having access only to VMs or virtual networks cannot be used to monitor this class of firewalls and (b) Some of the implementations of this class of firewall support only 5-tuple based rules (Source and Destination IP Address, Source and Destination Ports and Protocol). They do not support higher level abstractions such as Security Groups, Zones or Containers. However, some of the latest offerings do support firewall rules based On higher level abstractions and flow statistics as well.

IV. SUMMARY & CONCLUSIONS

In this paper, we performed a detailed analysis of two network segmentation approaches and two virtual firewall types for the protection of VMs in virtualized infrastructures. Comparing the features of the two network segmentation techniques, we find that the only distinct advantage that overlay-based network segmentation (such as VXLAN) holds over the VLAN-based approach is its infinite scalability. Hence, unless the number of VMs in the data center is in the order of thousands, the VLAN-based approach provides a satisfactory outcome in terms of performance and for meeting the goal of securing VMs. Because of this, the VLAN approach is economically justifiable in many environments. Further justification comes from the fact that overlay-based network segmentation schemes require sophisticated virtual switches, large mapping tables and the overhead of creating a control plane using SDN controllers.

Analyzing the relative advantages and disadvantages of the two firewall types – VM-based and hypervisor kernel-based – we find that the hypervisor kernel-based firewall is superior to the VM-based one in terms of three features. They are: (a) Performance (executes in the hypervisor kernel instead of in a VM), (b) Reduced network traffic (no diversion of traffic needed from various switches to the VM hosting the firewall) and, (c) Firewall rules are associated with the VM interface (since it is placed between a VM NIC and the virtual switch) and move with VM. The third feature is very critical from the point of view of the security of the VM, since it provides continued protection to it even when it migrates to different virtualized hosts or host clusters within the data center, without any additional re-configuration. It is this overwhelming security assurance feature that makes the hypervisor kernel-based firewall, the security software of choice in many virtualized infrastructures.

REFERENCES

[1] D. Shackleford, Virtualization Security – Protecting Virtualized Environments, Wiley Publishing Inc, Indianapolis, IA, USA, 2013

[2] "DMZ Virtualization with VMware Infrastructure". [Online]. http://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf [retrieved: Jan, 2016].

[3] "MAC Bridges and Virtual Bridged LANs". [Online]. https://www.ietf.org/meeting/86/tutorials/86-IEEE-8021-Thaler.pdf [retrieved: Dec, 2015].

[4] "IEEE 802.1Q Virtual LANs (VLANs)". [Online]. http://www.ieee802.org/1/pages/802.1Q.html [retrieved: Dec, 2015].

[5] A. Hameed, and A. N. Mian, "Finding Efficient VLAN Topology for better broadcast containment," Third International Conference on the Network of the Future (NOF), Gammarth, Nov 2012, pp.1-6.

[6] Introduction to Virtualized Networking. [Online]. http://www.ipspace.net/Introduction_to_Virtualized_Networking [retrieved: Dec, 2015].

[7] Overlay Virtual Networking. [Online]. http://www.ipspace.net/Overlay_Virtual_Networking [retrieved: Dec, 2015].

Copyright (c) The Government of USA, 2016. Used by permission to IARIA. ISBN: 978-1-61208-460-2

[8] “Overlay Virtual Networking and SDDC”. [Online]. http://my.ipspace.net/bin/list?id=xSDNOverlay [retrieved: Jan, 2016].

[9] “Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks”. [Online]. https://tools.ietf.org/html/rfc7348 [retrieved: Jan, 2016].

[10] “VXLAN Overview: Cisco Nexus 9000 Series Switches”. [Online]. http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-729383.pdf [retrieved: Dec, 2015].

[11] “Scaling Overlay Virtual Networks”. [Online]. http://content.ipspace.net/get/Scaling%20Overlay%20Virtual%20Networks.pdf [retrieved: Jan, 2016].

[12] Virtual Firewalls. [Online]. http://www.ipspace.net/Virtual_Firewalls [retrieved: Dec, 2015].

[13] Virtual Firewall. [Online]. https://en.wikipedia.org/wiki/Virtual_firewall [retrieved: Dec, 2015].

Copyright (c) The Government of USA, 2016. Used by permission to IARIA. ISBN: 978-1-61208-460-2

Software-defined Radio Based Measurement Platform for Wireless Networks

I-Chun Chao* Kang B. Lee† Richard Candell† Frederick Proctor† Chien-Chung Shen‡ Shinn-Yan Lin**
*Department of Electrical Engineering, National Taiwan University, Taiwan
†Networked Control Systems Group, National Institute of Standards and Technology, USA
‡Department of Computer and Information Sciences, University of Delaware, USA
**Telecommunication Laboratories, Chunghwa Telecom Company Ltd., Taiwan

***Abstract*—End-to-end latency is critical to many distributed applications and services that are based on computer networks. There has been a dramatic push to adopt wireless networking technologies and protocols (such as WiFi, ZigBee, WirelessHART, Bluetooth, ISA100.11a, *etc.*) into time-critical applications. Examples of such applications include industrial automation, telecommunications, power utility, and financial services. While performance measurement of wired networks has been extensively studied, measuring and quantifying the performance of wireless networks face new challenges and demand different approaches and techniques. In this paper, we describe the design of a measurement platform based on the technologies of software-defined radio (SDR) and IEEE 1588 Precision Time Protocol (PTP) for evaluating the performance of wireless networks.**

***Key words*—**Software-defined Radio, IEEE 1588 Precision Time Protocol, end-to-end latency, hardware time-stamp, out-of-band method

I. Introduction

End-to-end latency is critical to many distributed applications and services that are based on computer networks. Examples of such applications include industrial automation, telecommunications, power utility, and financial services. In particular, the capability of precise timing and time synchronization is of paramount importance for industrial control networks [1]. In addition, for applications such as Voice over Internet Protocol (VoIP) and stream videos, correct timing behaviors are extremely important to their (perceived) performance. As traditional applications can tolerate tens of milliseconds of end-to-end latency, modern real-time precision control and algorithmic trading are sensitive to latency of microseconds or even sub-microsecond. Given the growing demands for lower latency, higher time resolution, and more accurate timing, it becomes essential to measure end-to-end latency with such precision and accuracy.

At the same time, there has been a dramatic push to adopt wireless networking technologies and protocols (such as WiFi, ZigBee, WirelessHART, Bluetooth, ISA100.11a, *etc.*) into industrial control networks [2], [3]. There are two main reasons for such a development. One is the cabling (both material and labor) cost. For instance, a reasonable power utility management system typically includes thousands of measured relay nodes, and the use of any wired technology such as Ethernet will incur high wiring and installation costs [4]. In addition to the cabling cost, there are applications and scenarios that render any wired configuration and deployment infeasible, such as mobile nodes and nodes operating in hazardous environments. In such cases, wireless technologies and autonomous deployment are the only feasible options.

While performance measurement of wired networks has been extensively studied, measuring and quantifying the performance of wireless networks face new challenges and demand different approaches and techniques. For instance, disturbances or noise affecting timing precision incurred during wireless communications should be mitigated as much as possible. One major component of the disturbances is incurred in either the Medium Access Control (MAC) or the Physical (PHY) layer of the protocol stack. It has been argued that so long as the performance metrics, such as one-way delay and jitter, can be precisely measured in the lower protocol layers, performance evaluation at the higher layers, such as quality of service and real-time constraints, can be facilitated [5].

In addition, although the activity of performance measurement for both wired networks and wireless networks shares certain common concerns (*e.g.*, real-time response and determinism), wireless networks impose additional challenges (*e.g.*, multi-path fading and Inter-Symbol Interference (ISI)). Therefore, how to precisely measure the arrival time (or the departure time) of a packet becomes the fundamental issue of getting precise time information in wireless networks.

There exist efforts such as [4] that used hybrid networks to achieve time synchronization between wired and wireless networks, and [6] that applied Network Time Protocol (NTP) to measure the time information between nodes in wireless networks. These efforts are based on the technique of software time-stampers. In comparison to hardware time-stampers [7], these solutions result in either imprecise synchronization performance or coarse accuracy on time-related parameters (*e.g.*, jitter and latency).

In this paper, we describe the design of a measurement platform based on the technologies of software-defined radio (SDR) and IEEE 1588 Precision Time Protocol (PTP) for measuring and evaluating the performance of wireless networks (including wireless sensor networks). By evaluating the performance metrics described in the paper, application behaviors based on robust time synchronization could be better quantified and evaluated.

We proceed in the next section to describe the GNU

Chao, I-Chun; Lee, Kang; Candell, Richard; Proctor, Frederick; Shen, Chien-Chung.
"Software-defined Radio Based Measurement Platform for Wireless Networks."
Paper presented at the 2015 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication, Beijing, China, Oct 11-Oct 16, 2015.

Radio software-defined radio platform and the accompanying Universal Software Radio Peripheral (USRP). The SDR-based measurement platform is described in Section III. Section IV describes the software timestamping mechanism implemented in the IEEE 802.11 WiFi protocol and the IEEE 802.15.4 ZigBee protocol, respectively. Section V depicts the hardware platform used to prototype the timestamping mechanism. Demonstrations of running the wireless protocols of WiFi and ZigBee to generate timestamps are also presented. The proposed implementation of a hardware Time-Stamping Unit (TSU) within the Field Programmable Gate Array (FPGA) of USRP is described in Section VI[1]. Section VII concludes the paper with future research activities.

II. Overview of GNU Radio and USRP

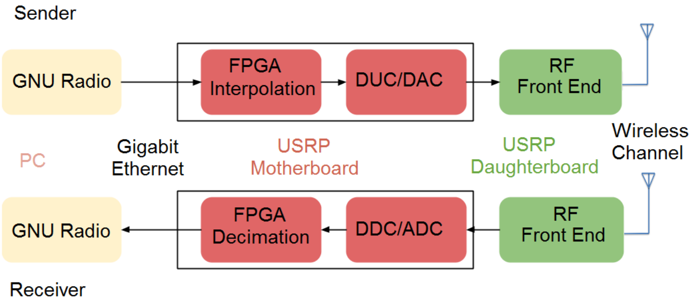
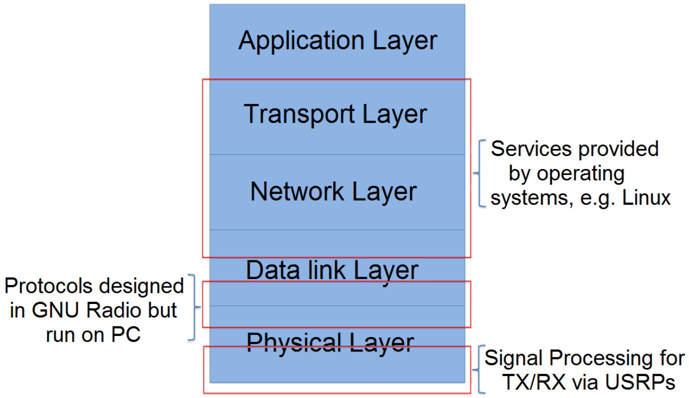


Fig. 1. Wireless communications with GNU Radio and USRP

GNU Radio is a collection of open source software which includes most wireless protocols and necessary modules for radio engineering and signal processing. The physical wave signals transmitted and received are defined by software and implemented on USRPs. Fig. 1 depicts how USRP and GNU Radio work together. The GNU Radio software library only executes on the personal computer (PC), and the USRP motherboard consists of some functionality in hardware, such as signal interpolation/decimation, Analog-to-Digital Converter (ADC)/Digital-to-Analog Converter (DAC), as well as Digital Up Converter (DUC)/Digital Down Converter (DDC). Furthermore, for transmission and reception in different frequency bands, different choices of daughterboards become necessary. For example, if we are conducting an experiment for 802.11 in the 2.4 GHz band, a specific daughterboard for operating in 2.3-2.9 GHz is required. Fig. 2 depicts the roles that both USRPs and GNU Radio play in a Transmission Control Protocol/Internet Protocol (TCP/IP) stack.

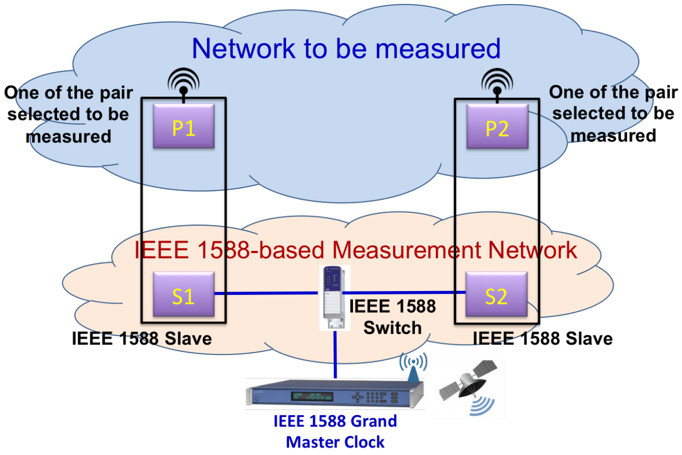


Application Layer
Transport Layer
Network Layer
Data link Layer
Physical Layer
Services provided by operating systems, e.g. Linux
Protocols designed in GNU Radio but run on PC
Signal Processing for TX/RX via USRPs

Fig. 2. The roles of GNU Radio and USRP in the TCP/IP stack

SDR is the other critical technology used in our proposed platform. In the following, we introduce the specific SDR platform, USRP and GNU Radio, we propose to use in our design. USRP is a platform for developing software radios, which has been developed in both computer-hosted form and embedded form. For this project, we choose the computer-hosted form. USRPs are controlled with open source drivers USRP Hardware Driver (UHD) and connected to a PC (for computer-hosted form) with either a Universal Serial Bus (USB) or a Gigabit Ethernet link so that radio protocols or algorithms can be designed and executed on a PC while the data are transmitted and received by the USRPs. USRPs are usually developed with the GNU Radio software suite to design complex software-defined radio systems. We selected one of the X series, USRP X310, as the platform for our testbed, which provides higher dynamic range and bandwidth, as well as a Multiple Input Multiple Output (MIMO) expansion port.

III. Measurement Platform



Network to be measured
One of the pair selected to be measured
P1
P2
One of the pair selected to be measured
IEEE 1588-based Measurement Network
S1
S2
IEEE 1588 Switch
IEEE 1588 Slave
IEEE 1588 Slave
IEEE 1588 Grand Master Clock

Fig. 3. Architecture of measurement platform

In this section, we describe the architecture of the proposed measurement platform and how we evaluate the results. The section is divided into (1) system architecture, (2) the design

[1] Implementation of the hardware TSU has not been completed yet. We present a high level design with specific FPGA modules identified where the hardware TSU could be implemented.

of an Adapting Gateway (AG) (a wireless component using USRP and a wired component using syn1588® Peripheral Component Interconnect Express (PCIe) Network Interface Card (NIC), (3) integration of the wireless and the wired portions, (4) use of wireless communication protocols, and (5) performance measurements.

A. System Architecture

To evaluate the performance of wireless networks we focus on time-related metrics, such as one-way delay and jitter. To obtain precise measurement of such information, it is critical to obtain the precise timestamp of packet arrivals and departures in the appropriate protocol layer(s). Fig. 3 presents the architecture which also depicts how the measurements are performed.

The idea depicted in Fig. 3 is to evaluate any two nodes in a wireless network (the upper network) with a condition that the two nodes are synchronized by using a synchronization network (the lower network). In the architecture, there are two networks and each plays a different role. The upper network is the target wireless network to be measured, termed WNUM (Wireless Network Under Measurement). Any pair of measured nodes (*e.g.*, P1 and P2 in the Fig. 3) in the WNUM may be selected and the performance such as latency, jitter, and one-way delay between the nodes may be obtained. The lower network is a PTP-based synchronization network responsible for synchronizing the clocks on the selected pair of nodes in the WNUM to a grand master traceable to, for instance, GPS (Global Positioning System) time.

In the PTP-based synchronization network, slaves (S1 and S2) selected to perform synchronization are actually part of their respective Adapting Gateways, which adapt an Ethernet network to a specific wireless network. For example, a gateway for measuring the performance of a ZigBee network is an Ethernet-ZigBee AG. The reason why measured nodes and slave nodes need to be integrated into one device is our proposed use of IEEE 1588 to synchronize S1 and S2. IEEE 1588 can guarantee the synchronization performance within sub-microsecond or less over Ethernet, so the arrival time and the departure time of each packet delivered from one end of the selected pair to the other end can be precisely measured. This specific AG for measuring wireless networks will be designed as depicted in Fig. 4. Inside the AG, there is a clock, which should be with high enough quality such as Oven-Controlled Crystal Oscillator (OCXO). This clock, located on the syn1588 PCIe NIC, will be synchronized to a grand master using IEEE 1588 via the syn1588 PCIe NIC, and, in the meantime, be a time source for drawing precise timestamps through USRP. In Fig. 4, we only consider one direction, either in a transmission or a reception. If the measurement requirements demand both directions, due to the asymmetric propagations of wireless communications, two antennas with daughterboards on each USRP become necessary.

B. Adapting Gateway (AG)

The functionality of AG can be divided into two components: one module to connect a wireless network (WNUM) and one to connect an Ethernet network (an PTP-based synchronization network).

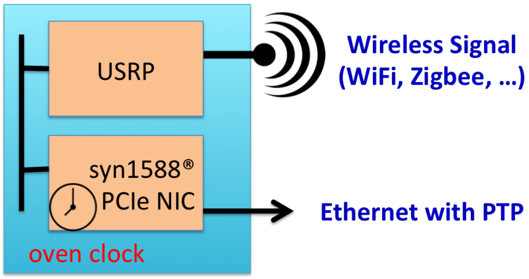


Fig. 4. Adapting gateway (AG)

1) Design of AG at wireless portion by using USRP: A USRP X310 is connected to a PC and equipped with two SBX 400-4400 MHz Rx/Tx daughterboards for receiving and transmitting wireless signal in the 400-4400 MHz band. Popular wireless technologies such as WiFi and ZigBee operate in this band. By programming new FPGA hardware modules for generating hardware timestamps while converting baseband signals to digital format, the customized USRP X310 also functions as a precise hardware time-stamper for the events of the packet arrival and departure in a wireless network.

2) Design of AG at wire portion by using syn1588 PCIe NIC: Since the clock on an AG directly affects the quality of the timestamp that USRP generates, synchronization between the node pair selected for measurement is extremely important. We use PTP to meet the necessary synchronization between the clocks on the chosen node pair in the WNUM. One syn1588 PCIe NIC plays the role of synchronizing to a grand master with PTP. Based on the results of our preliminary work, synchronization can achieve a precision on the order of hundred-nanosecond or better.

3) Integration of wireless and wired portions: However, two issues arise when a wired portion and a wireless portion are integrated. One issue is how USRP X310 and syn1588 PCIe NIC can share the same clock in an AG, and the other is how to coordinate these two components in a consistent manner. We propose to develop a software-based solution using Inter-Process Communication (IPC). There will be four processes running in Linux on the host computer to access both USRP X310 and syn1588 PCIe NIC, respectively. The first process, written with GNU Radio in Python, implements certain targeted protocols, *e.g.*, 802.11, ZigBee, etc. The second process accesses syn1588 PCIe NIC so that the internal OCXO can be precisely synchronized to a grandmaster. The third process draws timestamp information from the USRP X310. The last process will be an application program for accessing timestamp information on the two nodes of the selected pair in WNUM, so as to generate the performance indices of latency, jitter, and one-way delay to evaluate the WNUM.

IV. Software Timestamping in GNU Radio Wireless Protocols

In this section, we identify the specific blocks in the signal flow graphs where the software timestamping mechanism is implemented for WiFi and ZigBee, respectively. All these flow graphs were created with the GNU Radio Companion (GRC), a graphical user interface to GNU Radio.

A. IEEE 802.11 WiFi

Figs. 5 and 6 are the signal flow graphs

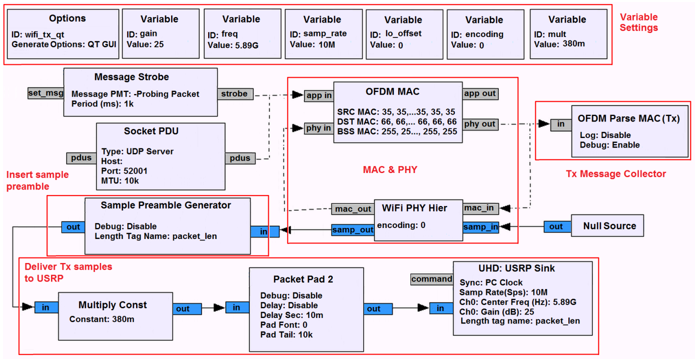


Fig. 5. Flow graph of IEEE 802.11 Tx Path

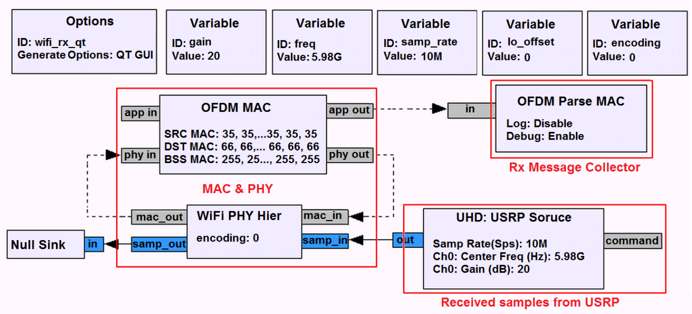


Fig. 6. Flow graph of IEEE 802.11 Rx path

B. IEEE 802.15.4 ZigBee

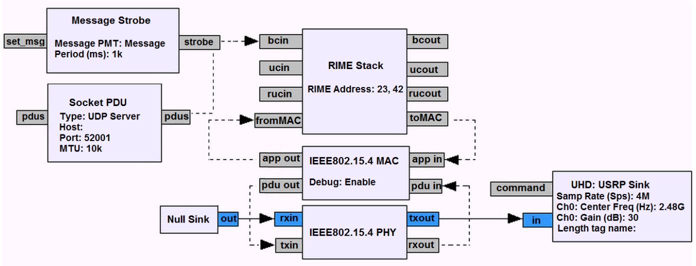


Fig. 7. Flow graph of IEEE 802.15.4 (ZigBee) Tx path

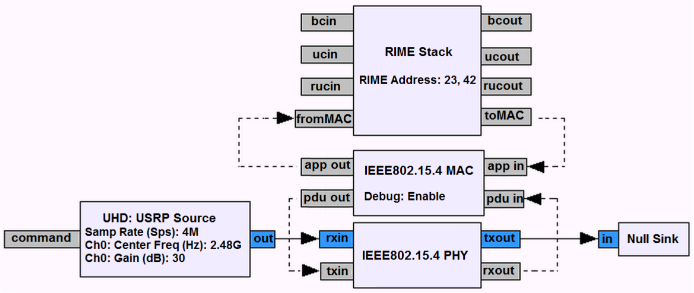


Fig. 8. Flow graph of IEEE 802.15.4 (ZigBee) Rx path

V. Timestamping Testbed and Demonstration

Fig. 9 and Fig. 10 depict the execution traces of timestamp generation while communicating via the IEEE 802.11 WiFi protocol and the IEEE 802.15.4 ZigBee protocol, respectively. For WiFi Tx, timestamps are generated in the block of “OFDM Parse MAC” of both Tx and Rx nodes. For ZigBee, timestamps are generated in the block titled “IEEE802.15.4 MAC” in both the Tx and Rx nodes.

VI. Hardware TSU in the USRP’s FPGA

Conceptually, hardware TSUs should be implemented, along the signal path, as close to the physical network interface (to the connection wire for wired networks or to the antenna for wireless networks) as possible to mitigate timing uncertainty. In the context of USRP, this is depicted by the two red arrows in Fig. 11, one before the digital upconversion (DUC) step in the transmitter chain and the other after the digital downconversion (DDC) step in the receiver chain.

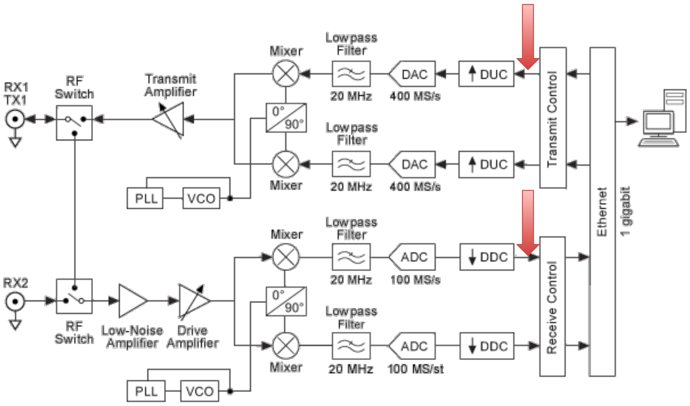
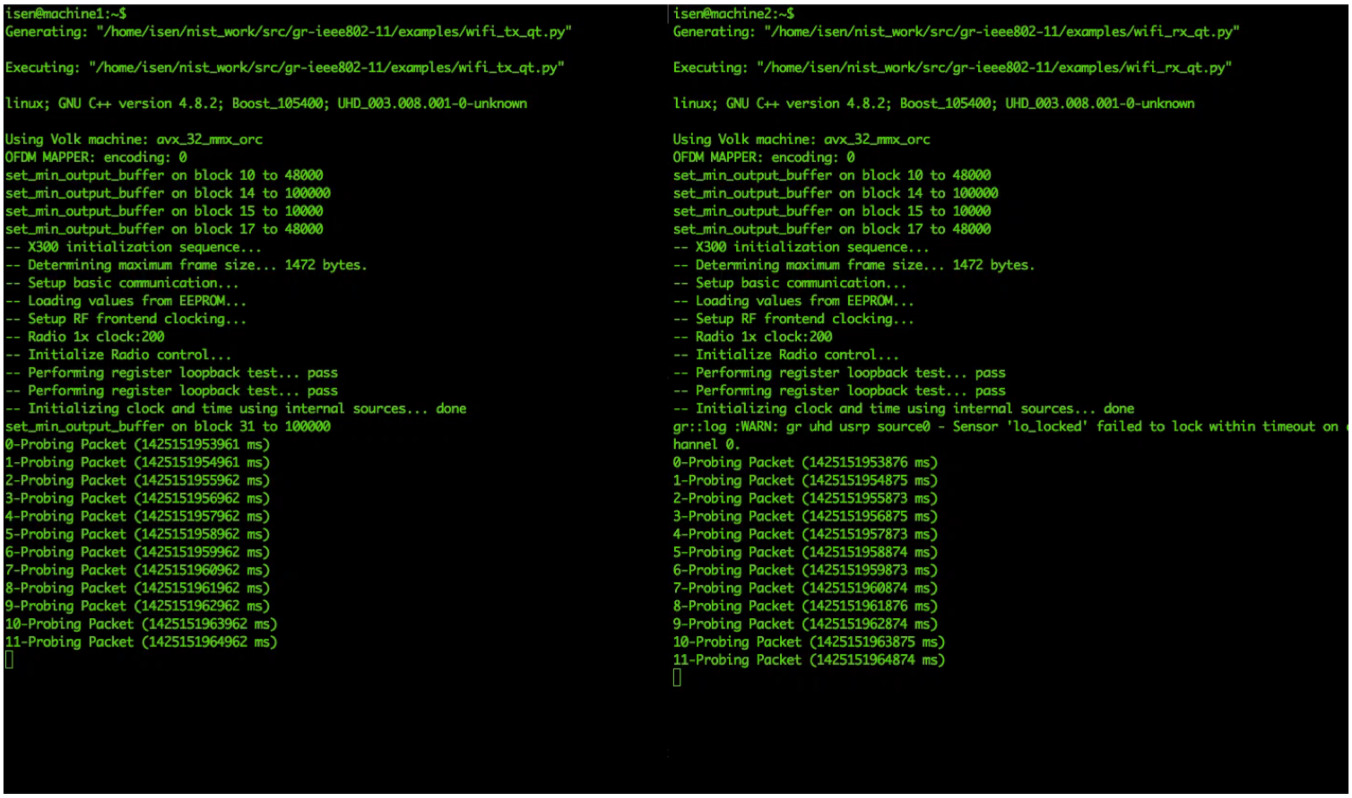


Fig. 11. Conceptual location of hardware TSU in USRP [8]

Since both DUC and DDC are implemented in the FPGA on the USRP, the two red arrows in Fig. 12 correspond to the two in Fig. 11 and depict the locations of the hardware TSUs inside the FPGA of the USRP X310. Specifically, we propose to develop (1) the *Tx TSU module* in-between the two existing FPGA modules `new_tx_control` and `duc_chain`, and (2) the *Rx TSU module* in-between the two existing FPGA



```
isen@machine1:~$
Generating: "/home/isen/nist_work/src/gr-ieee802-11/examples/wifi_tx_qt.py"

Executing: "/home/isen/nist_work/src/gr-ieee802-11/examples/wifi_tx_qt.py"

linux; GNU C++ version 4.8.2; Boost_105400; UHD_003.008.001-0-unknown

Using Volk machine: avx_32_mmx_orc
OFDM MAPPER: encoding: 0
set_min_output_buffer on block 10 to 48000
set_min_output_buffer on block 14 to 100000
set_min_output_buffer on block 15 to 10000
set_min_output_buffer on block 17 to 48000
-- X300 initialization sequence...
-- Determining maximum frame size... 1472 bytes.
-- Setup basic communication...
-- Loading values from EEPROM...
-- Setup RF frontend clocking...
-- Radio 1x clock:200
-- Initialize Radio control...
-- Performing register loopback test... pass
-- Performing register loopback test... pass
-- Initializing clock and time using internal sources... done
set_min_output_buffer on block 31 to 100000
0-Probing Packet (1425151953961 ms)
1-Probing Packet (1425151954961 ms)
2-Probing Packet (1425151955962 ms)
3-Probing Packet (1425151956962 ms)
4-Probing Packet (1425151957962 ms)
5-Probing Packet (1425151958962 ms)
6-Probing Packet (1425151959962 ms)
7-Probing Packet (1425151960962 ms)
8-Probing Packet (1425151961962 ms)
9-Probing Packet (1425151962962 ms)
10-Probing Packet (1425151963962 ms)
11-Probing Packet (1425151964962 ms)
```

```
isen@machine2:~$
Generating: "/home/isen/nist_work/src/gr-ieee802-11/examples/wifi_rx_qt.py"

Executing: "/home/isen/nist_work/src/gr-ieee802-11/examples/wifi_rx_qt.py"

linux; GNU C++ version 4.8.2; Boost_105400; UHD_003.008.001-0-unknown

Using Volk machine: avx_32_mmx_orc
OFDM MAPPER: encoding: 0
set_min_output_buffer on block 10 to 48000
set_min_output_buffer on block 14 to 100000
set_min_output_buffer on block 15 to 10000
set_min_output_buffer on block 17 to 48000
-- X300 initialization sequence...
-- Determining maximum frame size... 1472 bytes.
-- Setup basic communication...
-- Loading values from EEPROM...
-- Setup RF frontend clocking...
-- Radio 1x clock:200
-- Initialize Radio control...
-- Performing register loopback test... pass
-- Performing register loopback test... pass
-- Initializing clock and time using internal sources... done
gr::log :WARN: gr uhd usrp source0 - Sensor 'lo_locked' failed to lock within timeout on 
hannel 0.
0-Probing Packet (1425151953876 ms)
1-Probing Packet (1425151954875 ms)
2-Probing Packet (1425151955873 ms)
3-Probing Packet (1425151956875 ms)
4-Probing Packet (1425151957873 ms)
5-Probing Packet (1425151958874 ms)
6-Probing Packet (1425151959873 ms)
7-Probing Packet (1425151960874 ms)
8-Probing Packet (1425151961876 ms)
9-Probing Packet (1425151962874 ms)
10-Probing Packet (1425151963875 ms)
11-Probing Packet (1425151964874 ms)
```

Fig. 9. Timestamping demonstration over IEEE 802.11 (WiFi)

modules new_rx_framer and ddc_chain_x300 to generate the Tx and Rx timestamps, respectively.

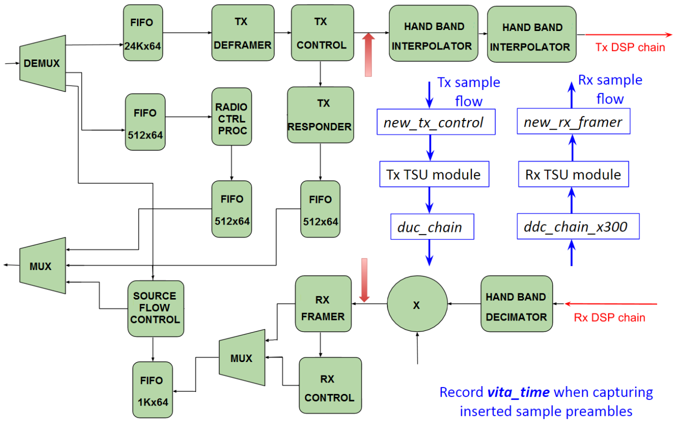


Fig. 12. Proposed location of hardware TSU in USRP's FPGA

To know the exact time at which to generate timestamps, we need a "triggering" mechanism that causes the *Tx TSU module* to generate a timestamp when a packet is about to be transmitted. Similarly, by recognizing the triggering condition for an incoming packet, the *Rx TSU module* generates the arrival timestamp. In our implementation, a *Sample preamble* is added, by the Sample Preamble Generator block in Fig. 5, before the Orthogonal Frequency-Division Multiplexing (OFDM) preamble of each outgoing packet, as depicted in Fig. 13. By recognizing the Sample preamble of an incoming packet, an Rx timestamp is generated.

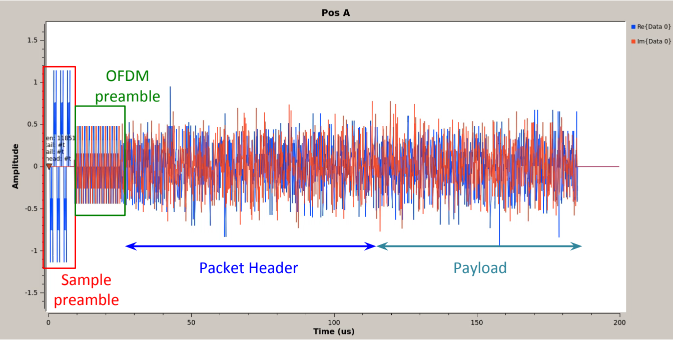
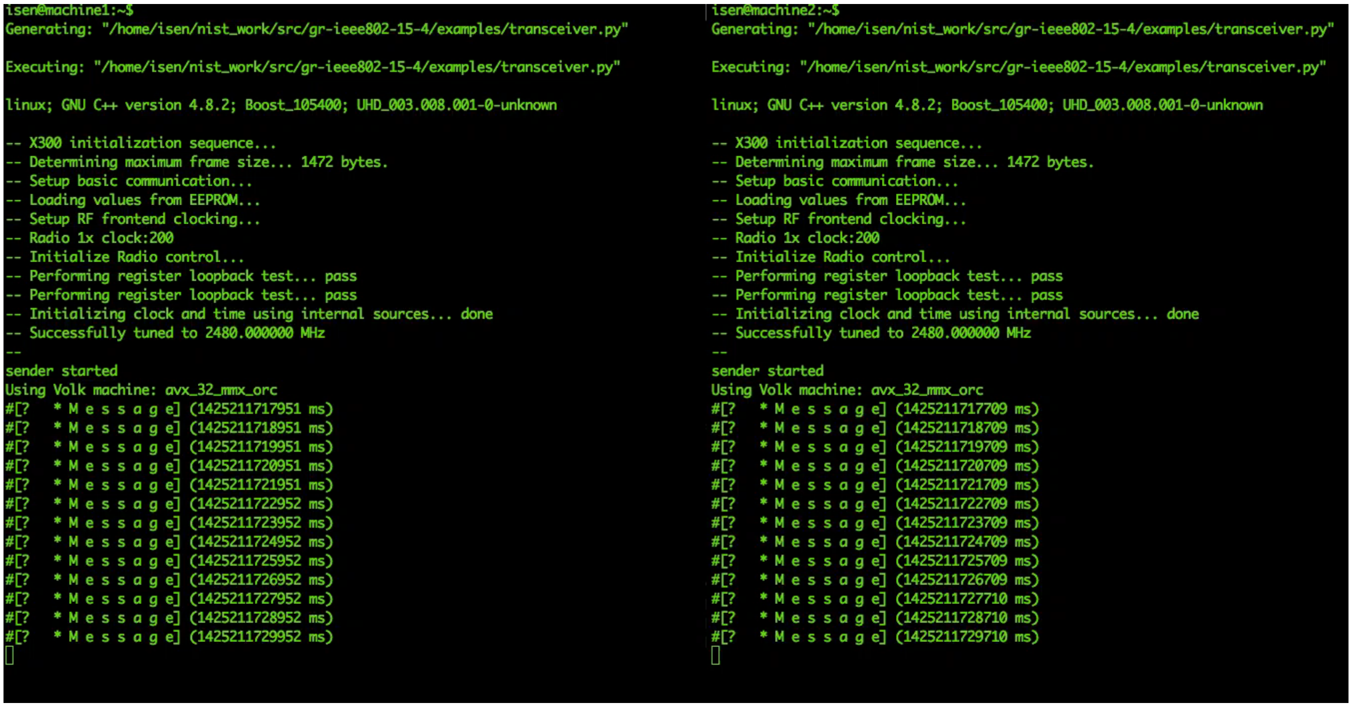


Fig. 13. Adding sample preamble before OFDM preamble

VII. Conclusion

In this paper, we describe a measurement platform based on the technologies of software-defined radio (SDR) and IEEE 1588 Precision Time Protocol (PTP) for measuring and evaluating the performance of wireless networks (including wireless sensor networks). By evaluating the performance metrics described in the paper, application behaviors based on robust time synchronization could be better quantified and evaluated. Work is in progress to complete the implementaion of the hardware timestmper inside the FPGA of USRP X310.



```
isen@machine1:~$
Generating: "/home/isen/nist_work/src/gr-ieee802-15-4/examples/transceiver.py"

Executing: "/home/isen/nist_work/src/gr-ieee802-15-4/examples/transceiver.py"

linux; GNU C++ version 4.8.2; Boost_105400; UHD_003.008.001-0-unknown

-- X300 initialization sequence...
-- Determining maximum frame size... 1472 bytes.
-- Setup basic communication...
-- Loading values from EEPROM...
-- Setup RF frontend clocking...
-- Radio 1x clock:200
-- Initialize Radio control...
-- Performing register loopback test... pass
-- Performing register loopback test... pass
-- Initializing clock and time using internal sources... done
-- Successfully tuned to 2480.000000 MHz
--
sender started
Using Volk machine: avx_32_mmx_orc
#[?   * M e s s a g e] (1425211717951 ms)
#[?   * M e s s a g e] (1425211718951 ms)
#[?   * M e s s a g e] (1425211719951 ms)
#[?   * M e s s a g e] (1425211720951 ms)
#[?   * M e s s a g e] (1425211721951 ms)
#[?   * M e s s a g e] (1425211722952 ms)
#[?   * M e s s a g e] (1425211723952 ms)
#[?   * M e s s a g e] (1425211724952 ms)
#[?   * M e s s a g e] (1425211725952 ms)
#[?   * M e s s a g e] (1425211726952 ms)
#[?   * M e s s a g e] (1425211727952 ms)
#[?   * M e s s a g e] (1425211728952 ms)
#[?   * M e s s a g e] (1425211729952 ms)
```

```
isen@machine2:~$
Generating: "/home/isen/nist_work/src/gr-ieee802-15-4/examples/transceiver.py"

Executing: "/home/isen/nist_work/src/gr-ieee802-15-4/examples/transceiver.py"

linux; GNU C++ version 4.8.2; Boost_105400; UHD_003.008.001-0-unknown

-- X300 initialization sequence...
-- Determining maximum frame size... 1472 bytes.
-- Setup basic communication...
-- Loading values from EEPROM...
-- Setup RF frontend clocking...
-- Radio 1x clock:200
-- Initialize Radio control...
-- Performing register loopback test... pass
-- Performing register loopback test... pass
-- Initializing clock and time using internal sources... done
-- Successfully tuned to 2480.000000 MHz
--
sender started
Using Volk machine: avx_32_mmx_orc
#[?   * M e s s a g e] (1425211717709 ms)
#[?   * M e s s a g e] (1425211718709 ms)
#[?   * M e s s a g e] (1425211719709 ms)
#[?   * M e s s a g e] (1425211720709 ms)
#[?   * M e s s a g e] (1425211721709 ms)
#[?   * M e s s a g e] (1425211722709 ms)
#[?   * M e s s a g e] (1425211723709 ms)
#[?   * M e s s a g e] (1425211724709 ms)
#[?   * M e s s a g e] (1425211725709 ms)
#[?   * M e s s a g e] (1425211726709 ms)
#[?   * M e s s a g e] (1425211727710 ms)
#[?   * M e s s a g e] (1425211728710 ms)
#[?   * M e s s a g e] (1425211729710 ms)
```

Fig. 10. Timestamping demonstration over IEEE 802.15.4 (ZigBee)

Acknowledgment

The work is supported in part by National Institute of Standards and Technology (NIST) Cooperative Agreement #70NANB14H087.

Disclaimer

No approval or endorsement of any commercial product by the National Institute of Standards and Technology is intended or implied. Certain commercial equipment, instruments, or materials are identified in this paper in order to facilitate understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose. This publication was prepared by United States Government employees as part of their official duties and is, therefore, a work of the U.S. Government and not subject to copyright.

References

[1] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," *IEEE Comm. Surveys & Tutorials*, vol. 15, no. 2, pp. 860–880, Second Quarter 2013.

[2] A. Willig, "Recent and emerging topics in wireless industrial communications: A selection," *IEEE Transactions on Industrial Informatics*, vol. 4, no. 2, pp. 102–124, May 2008.

[3] J. R. Moyne and D. M. Tilbury, "The emergence of industrial control networks for manufacturing control, diagnostics, and safety data," *Proceedings of IEEE*, vol. 95, no. 1, pp. 29–47, January 2007.

[4] A. Mahmood and F. Ring, "Clock synchronization for IEEE 802.11 based wired-wireless hybrid networks using PTP," in *Proc. IEEE Int. Symp. Precision Clock Synchronization Meas., Control Commun.*, San Francisco, California, September 23-28 2012, pp. 1–6.

[5] A. Hernandez and E. Magana, "One-way delay measurement and characterization," in *Proc. 3rd International Conference on Networking and Services (ICNS)*, Athens, Greece, 2007, pp. 114–120.

[6] K. Stangherlin, R. C. Filho, W. Lautenschlager, V. Guadagnin, L. Balbinot, R. Balbinot, and V. Roesler, "One-way delay measurement in wired and wireless mobile full-mesh networks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, Cancun, Mexico, 2011, pp. 1044–1049.

[7] A. Mahmood and G. Gaderer, "Timestamping for IEEE 1588 based clock synchronization in wireless LAN," in *Proc. IEEE Int. Symp. Precision Clock Synchronization Meas., Control Commun.*, Brescia, Italy, 2009, pp. 1–6.

[8] "What Is NI USRP Hardware?" National Instruments, Tech. Rep., April 1 2015. [Online]. Available: http://www.ni.com/white-paper/12985/en/

Time Dependent Dielectric Breakdown in high quality SiC MOS capacitors

Zakariae Chbili[1,2] **,** Kin P. Cheung[1,a], Jason P. Campbell[1], Jaafar Chbili[1,2],Mhamed Lahbabi[3] , Dimitris E. Ioannou[2] and Kevin Matocha[4]

[1]NIST, 100 Bureau Dr, Gaithersburg, MD, 20899 USA

[2]George Mason University, 4400 Uiversity Dr, Fairfax, VA 22030 USA

[3]Laboratoire SSC, Faculté des Sciences et Techniques USMBA, B.P. 2202 Fez, Morocco

[4]Monolith Semiconductor Inc, 408 Fannin Av, Round Rock, TX 78664 USA

[a]Kin.Cheung@nist.gov

Keywords: Power electronics, SiC, MOS capacitors, Reliability, TDDB, Weibull distribution, Field acceleration and Activation energy.

Abstract. In this paper we report TDDB results on SiO_2/SiC MOS capacitors fabricated in a matured production environment. A key feature is the absence of early failure out of over 600 capacitors tested. The observed field accelerations and activation energies are higher than what is reported on SiO_2/Si of similar oxide thickness. The great improvement in oxide quality and the deviation from typical SiO_2/SiC observations are explained by the quality of the oxide in this study.

Introduction

Due to the better material properties of Silicon Carbide and the significant progress made by the SiC community in the last two decades, SiC power MOSFETs continue to gain acceptance in the power market and are considered the most prominent competitors to the widely used Si IGBT. The rapid expansion of the power market due to the implementation of clean and renewable energy also presents a unique opportunity for the SiC MOSFET. However, the integrity of the gate oxide remains an important concern for SiC MOSFET adoption.

SiC MOSFET gate oxide breakdown reliability as measured by Time Dependent Dielectric Breakdown (TDDB) has made great progress as the technology matures [1-6]. However, while the intrinsic breakdown reliability has be shown to be good enough [2-6], a persistent early failure tail of the breakdown distribution remains a tough nut to crack. When this tail exists, it determines the failure rate of the SiC MOSFET, not the intrinsic distribution and the resulting projection is not good. This is because reliability is about the low percentile failures, not the 63% failure time. An added challenge of this early failure distribution is that it can only be investigated properly with a large sample size. After all, one cannot say much about the 1% or less failure behavior without testing 100 devices or more. In this study, we report for the first time TDDB result with no early failure from over 600 SiC MOS capacitors. The extracted electric field and temperature accelerations from these devices are steeper than those observed in thick SiO_2 on silicon devices [7-12].

Experimental Setup

A home-built massively parallel reliability test system was used in this study in order to achieve the statistics required for high accuracy of TDDB lifetime projections [13] and to properly address the early failure distribution if exists. Fig. 1 shows the wafer level test system incorporating many miniaturized probe stations each with a testing capacity of 100 probe pins and all the associated source and measure electronics. They were designed to provide a stress voltage up to ± 200V and a stress temperature up to 400 C.

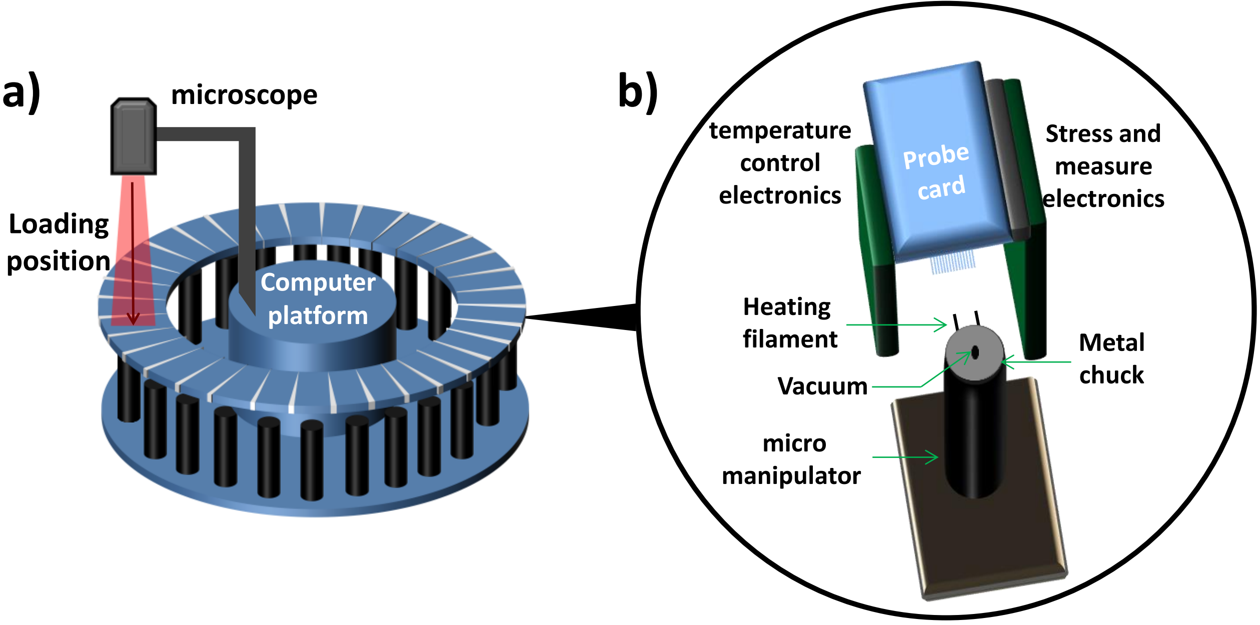


Fig. 1 a) Illustration of the massively parallel reliability system b) view of different units in a single station

TDDB data were collected from more than 600 nMOS SiC capacitors with a gate area of 40 x 250 um^2. The gate oxide is a thermally grown, 50 nm thick SiO_2 fabricated in a matured production environment. Fifteen different TDDB stress conditions (8.2 MV/cm - 9.5 MV/cm, substrate injection mode, and 150°C - 300°C) were applied to groups of 50 devices each.

Results and Discussions

Fig. 2 shows the cumulative failure distribution as a function of breakdown time for all measured devices in Weibull scale. While typical SiO_2/SiC TDDB failure distributions encompass a large number of early failures [4, 5] resulting in bi-modal failure distributions, the Weibull distributions observed here show no signs of early failure. We like to emphasize that no censoring has been done to the data in Fig. 2. This absence of extrinsic failures is observed for the first time – an important milestone for SiC MOSFET technology.

TDDB data from SiC devices is typically observed to be temperature independent over a wide range of temperatures [3, 5] and the activation energy is often reported to exhibit "extrinsic-induced" slope variations but remain field independent [2, 5, 6]. These observations are in agreement with the behaviors of SiO_2/Si system when the oxide is thick but not when the oxide is thinner [7-12].

In general, most TDDB data for thick oxide in both SiO_2/Si and SiO2/SiC systems show significant early failure populations. Such early failure population can seriously affect the extraction of characteristic lifetime as well as the extraction of the field

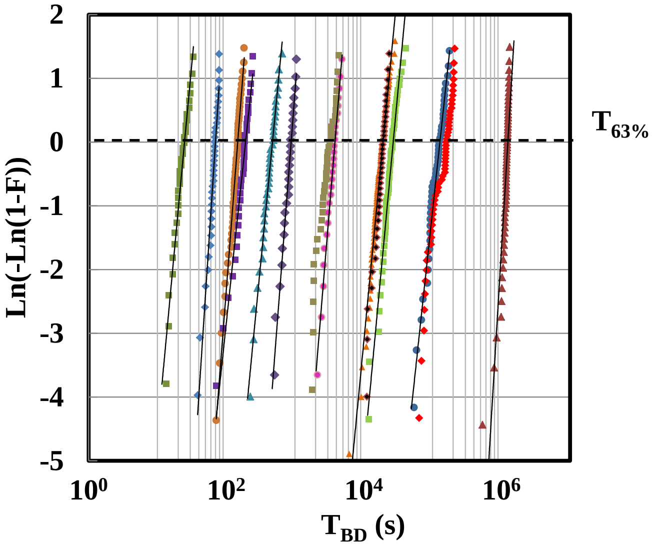


Fig. 2 Cumulative failure distributions for more than 600 SiC MOS capacitors showing no extrinsic failures (raw data)

dependent activation energy as well as the temperature dependent field acceleration of breakdown time. Using better quality samples, Kaczer et al. showed a clear oxide thickness effect on temperature acceleration [14]. It is expected that the effect of temperature should be weaker in thick oxide but not absence. Data shown in figure 2 is rare for thick oxide. The absence of early failure allows the temperature effect to be studied cleanly.

Fig. 3.a) shows the measured lifetimes at different stress fields and four different stress temperatures. In contrast to SiC TDDB data over the last decade, the field acceleration factor is clearly temperature dependent.

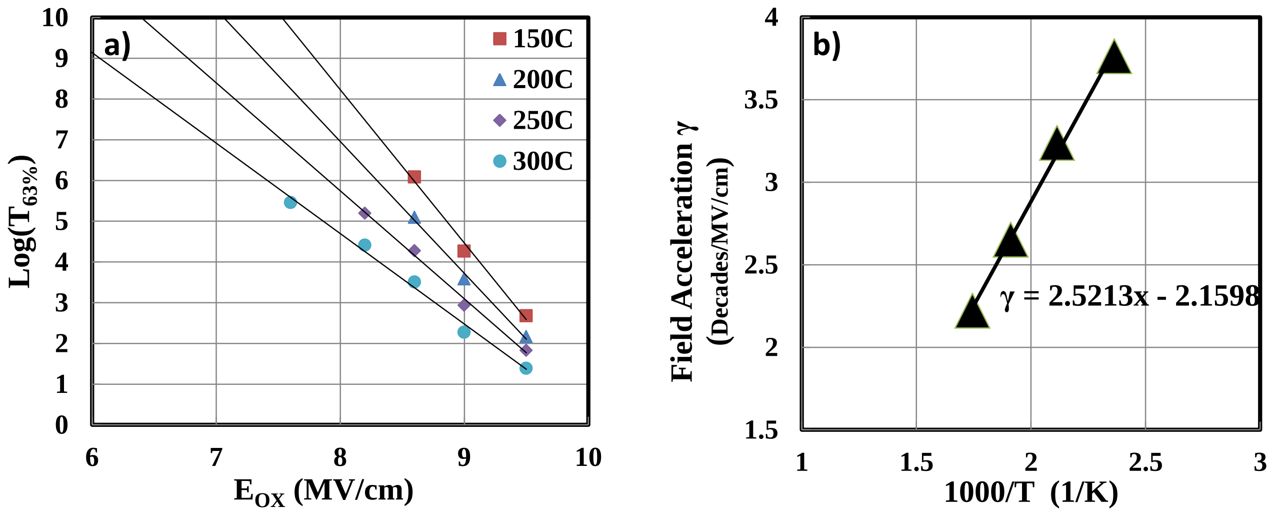


Fig. 3 a) Measured TDDB lifetime at different temperatures b) Corresponding field acceleration exhibiting temperature dependence (Not typically observed in SiC)

Fig. 3.b) shows the variation of the field acceleration with temperature. It is clearly linearly proportional to the inverse of the temperature (the linear fit is $\gamma = b/T + C$). The extracted slope of field acceleration is higher than the value reported for Si devices with much lower thickness [7]. Since thicker oxide is expected to have weaker temperature effect, this is a surprising result.

At 9 MV/cm and above, the recorded lifetime is comparable to reported for silicon devices [7-12]. The higher field acceleration, however, make the lifetime of our SiC device much longer than silicon devices at lower field. This is completely counter-intuitive because the electron tunneling barrier (from substrate for the stress conditions reported here) for SiC device is lower than Si device (2.7eV vs 3.1 eV), which should result in much shorter lifetimes. Given such results, our first order of business is to careful examine our test conditions to eliminate any possible experimental errors and we are sure that there are no experimental artefacts.

For characteristic lifetime extraction, proper treatment of the early failures is to model the whole data set as joint distributions [15]. However, this is almost never done for TDDB data of thick oxide in the literature [7-12]. Failure to do so seriously underestimates the true intrinsic lifetime. This is perhaps the main reason for the surprising result of our SiC device better than Si device in terms of breakdown lifetime.

Similar to temperature dependent field acceleration, field dependent temperature acceleration (or temperature activation energy) study can also benefit from the exceptionally clean data of figure 2.

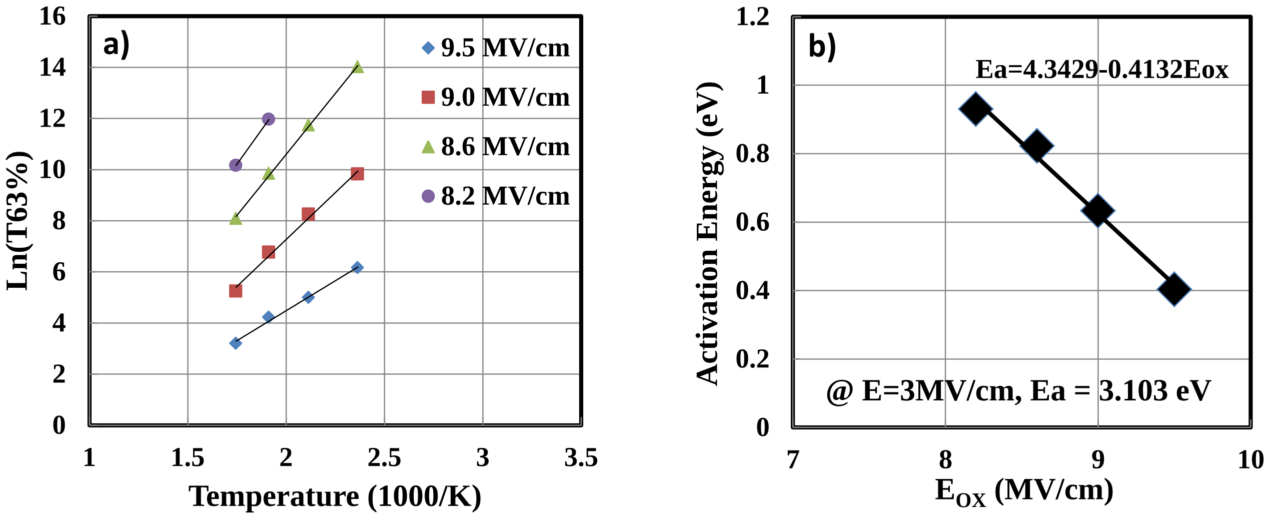


Fig. 4 a) Measured TDDB lifetime at different oxide fields b) Corresponding activation energy exhibiting field dependence (Not typically observed in SiC)

Fig. 4.a) shows the measured lifetimes at different stress temperatures and different fields. The change in slope at different stress fields is clearly illustrated in Fig. 4.b) where the field dependence of the activation energy is plotted. The activation energy of breakdown is reasonably linear to the oxide field. The extrapolation of the activation energy of breakdown into operation conditions results in an activation energy of breakdown of 3.1eV at E = 3 MV/cm. This is also rather high comparing to the silicon value [10]. These observations of strong temperature effect for our thick oxide samples are likely more than the result of clean data set. It is likely an intrinsic different between SiC substrate and Si substrate and further study is on-going.

Conclusion

TDDB with good statistics was performed on SiC MOS capacitors issued from a mature fabrication environment and no extrinsic failures were found in over 600 devices. The absence of early failure is a first time observation, at least for SiC MOS capacitors. The steep slope of field acceleration projects extremely high breakdown reliability at operation field even at 300C. Early failure is one of the few remaining obstacles in the road to SiC MOSFET commercial success. The proof that early failures can be largely eliminated, at least for capacitors, is a major milestone.

References

[1] M. M. Mathur et al., IEEE TED (1999) 520-524.
[2] M. K. Das et al., Mat. Sci. For., (2012), 717-720
[3] L. C. Yu et al, IIRW (2008), 141-144
[4] M. Gurfinkel et al., IEEE TDMR (2008) 635-641
[5] L. C. Yu et al., IEEE TDMR (2010), 418-426
[6] K. Matocha et al., IEEE TED (2008), 1830-1834
[7] A. Yassine et al. IEEE EDL (1999) 390-392
[8] E. Vincent et al., ESREF (1996) 1643-1646
[9] J. W. McPherson, IRPS (1986) 12-18
[10] J. S. Suehle et al. IIRW (1993) 59-67
[11] J. W. McPherson et al. JES (1985) 190-1908
[12] M. Kimura, IEEE TED (1999) 220-229
[13] Z. Chbili et al. IEEE IIRW (2015).
[14] B. Kaczer et al.,ESSDERC-99, pp356.
[15] J. L. Ogier et al., ESSDERC-95, pp299.

Chbili, Zakariae; Cheung, Kin; Campbell, Jason; Chbili, Jaafar; Lahbabi, Mhamed; Ioannou, D.; Matocha, Kevin.
"Time Dependent Dielectric Breakdown in high quality SiC MOS capacitors."
Paper presented at the Materials Science Forum, Giardini Naxos, Italy, Oct 4-Oct 9, 2015.

COVER SHEET

Title: *The performance of structural steel beams subject to a localized fire*

Authors[*]: Lisa Choe, Selvarajah Ramesh, Chao Zhang, John Gross

[*] National Institute of Standards and Technology, 100 Bureau Dr, Gaithersburg, Maryland 20899, USA
lisa.choe@nist.gov, selvarajah.ramesh@nist.gov, chao.zhang@nist.gov, john.gross@nist.gov

Choe, Lisa; Ramesh, Selvarajah; Zhang, Chao; Gross, John.
"The performance of structural steel beams subject to a localized fire."
Paper presented at the 9th International Conference on Structures in Fire SiF'16, Princeton, NJ, Jun 8-Jun 10, 2016.

(FIRST PAGE OF ARTICLE)

ABSTRACT

This paper presents the results from the open flame, localized fire tests conducted on 6.17 m long, simply supported W16×26 beam specimens. The cross sections at midspan (i.e., expected plastic hinge zone) of the beam specimen were directly exposed to the natural gas fire. Two different tests were conducted: (1) fire-thermal tests to evaluate the effects of the prescribed heat release rates (HRR), provided by the 1 m^2 natural gas burner, on the thermal responses of the specimen and (2) structural-fire test to evaluate the fire effects on the overall behavior and the load-bearing capacity of the specimen. The test results indicated that the prescribed heat release rates from the burner affected the heating rate of the specimen. When the HRR-time relationship of the burner followed a step function, the fire-exposed region of the beam specimen was heated essentially linearly with increasing time of fire exposure. When the HRR was set to a target magnitude of 400 kW throughout the test, the fire-exposed region was heated nonlinearly until it reached a steady-state temperature condition. When the beam specimen was subjected to linearly increasing flexural loads at a maintained HRR of 700 kW, combined flexural and lateral torsional failure of the specimen was exhibited. The lateral deformations in the compression flange at the fire-exposed critical sections initiated at (124 ± 5) kN-m, which is 39% of the plastic moment capacity at room temperature. The peak moment capacity was (171 ± 9) kN-m (54 % of the plastic moment capacity at room temperature), while the maximum temperature was (642 ± 28) ˚C at the HRR of 700 kW. The test results from the present study can be used for developing or calibrating analytical models, which can be eventually used for evaluating the performance of structural members subjected to a localized fire.

INTRODUCTION

The 6.17 m long W16×26 beam specimens subjected to a localized fire were tested at the National Fire Research Laboratory (NFRL) [1] of the National Institute of Standards and Technology (NIST). The main objective of these tests was to commission the structural fire experimental measurement capabilities of the newly constructed laboratory. A secondary objective was to generate data set for validation of analytical models. The experimental tests were divided into two parts: the fire-

Choe, Lisa; Ramesh, Selvarajah; Zhang, Chao; Gross, John.
"The performance of structural steel beams subject to a localized fire."
Paper presented at the 9th International Conference on Structures in Fire SiF'16, Princeton, NJ, Jun 8-Jun 10, 2016.

thermal tests and the structural-fire test. The fire-thermal tests were intended to evaluate temperature-time responses of the steel beam specimen exposed to an open flame, localized fire with controlled heat release rates (HRR). No structural load was applied except the self-weight of the beam specimen. The structural-fire test was conducted such that the flexural loads and the open flame fire were applied to the critical sections (i.e., expected plastic hinge zone) of the specimen to evaluate the behavior and the flexural strength of the simply supported steel beam specimen.

FIRE-THERMAL TEST

Test setup, test protocol, and instrumentation layout

Figure 1 shows the test setup under the exhaust hood (13.7 m ×15.2 m) in the NFRL structural fire test bay. The W16×26 beam specimen of ASTM A992 steel [2] was placed on seated connections which were bolted to the W12×106 reaction column assemblies. Nominal dimensions of the W16×26 and W12×106 shapes are provided in ANSI/AISC 360-10 [3]. The fuel delivery system consisted of two natural gas burners with a nominal flame zone of one square meter to provide heat release rate (HRR) up to 1.5 MW. The uncertainty in the HRR measurements with a natural gas burner is presented in Bryant et al. [4] and not presented here for brevity. The distance from the lower flange of the beam specimen to the strong floor was 1.6 m. The assembled burner was placed 1 m below the lower flange of the specimen.

To evaluate the thermal behavior of the beam specimen and the reproducibility of the fire test in the NFRL, five individual tests were conducted on the same specimen under two different fire conditions provided by the natural gas burner. The first series of the tests was conducted by increasing the heat release rate in 100 kW increments approximately every 5 min (Tests 1 and 2); the second series of the tests utilized the heat release rate fixed at 400 kW throughout the test period (Tests 3, 4, and 5). All of the five tests were terminated when any one of the thermocouples installed at the specimen indicated about 500 °C.

Test data included the heat release rate of the burner, temperatures, adiabatic surface temperatures (to characterize thermal exposure), and displacements of the beam specimen. For temperature measurements, a total of fifty-three, type-K, 24 gauge thermocouples (tc) were installed at eleven different cross sections along the specimen length as shown in Figure 1. Four 25 mm linear position sensors were installed at 0.29 m from the beam ends to measure the axial displacements (thermal elongation). Two 50 mm linear position transducers were used to measure the vertical displacement induced by thermal bowing effects. For tests 3 through 5, four plate thermometers were installed to measure the adiabatic surface temperature at midspan of the beam specimen. A thermal imaging camera was used to record the spatial temperature distribution in the fire-exposed portion of the beam specimen.

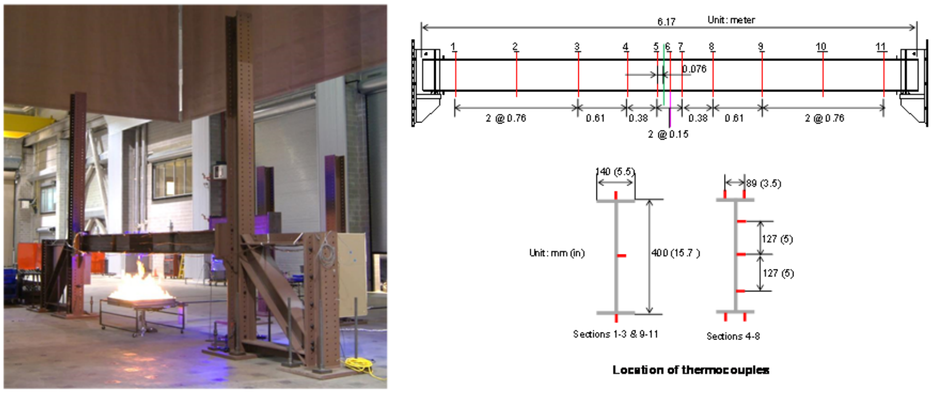


Figure 1. Fire-thermal test setup and thermocouple layout

Test results

Figure 2 shows the heat release rate output from the burner for each test and the corresponding temperature changes at the fire-exposed zone of the specimen. Temperatures shown herein are the average values tc readings across sections 5, 6, and 7 at five different locations through the section depth. Six thermocouple readings were used to obtain the average temperature of the upper and lower flange and three thermocouple readings were used for each web temperature in Figure 2. No permanent deformation of the beam specimen was observed in the heating or cooling phase of the fire.

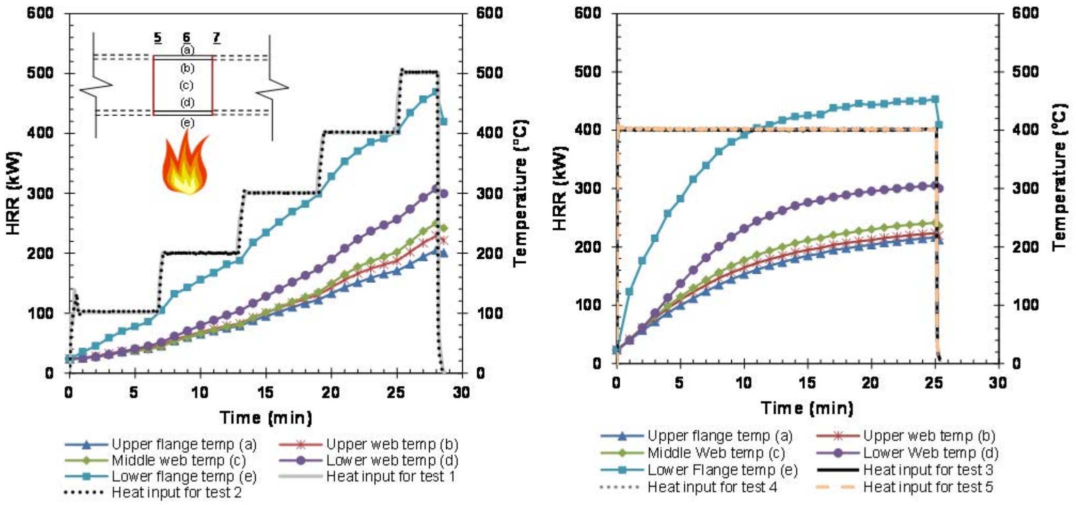


Figure 2. Heat input from the burner and steel temperatures at midspan[†]

When a step function was used to increase the heat source (i.e., HRR from the burner), it took approximately 28 min after ignition to reach the maximum discrete temperature of 500 °C at the lower flange of the specimen at midspan. The coefficient

[†] The estimated expanded uncertainty (*U*) of the temperature data is 20 °C (confidence interval of 95%) with *U* determined from a combined standard uncertainty (u_c = 10 °C) in the repeated temperature measurements at sections 5, 6, and 7 and the assumption that the possible estimated values of the standard are normally distributed with u_c.

of variation (COV) in the measured HRR from the two repeated tests (Tests 1 and 2) was 0.3%. The temperatures at the fire-exposed midspan of the beam specimen increased almost linearly until the fire was extinguished. A thermal gradient through the section depth was also exhibited. The temperature difference between the lower flange and the lower web (i.e., tc locations e and d, respectively, as shown in Figure 2) increased with increasing time of fire exposure, and reached 160 °C at 28 min. However, the maximum difference in temperatures at the upper portion of the cross section (along the tc locations a through c) remained below 25 °C.

When the burner was set to generate the constant HRR of 400 kW, it took approximately 25 min after ignition to reach the maximum discrete temperature of 500 °C at the lower flange of the specimen at midspan. The COV of the heat input from the three repeated tests (Tests 3, 4, and 5) was 0.2%. Unlike the previous tests, the temperatures at the exposed midspan of the specimen increased nonlinearly. The temperatures of the specimen increased rapidly following ignition, and then the rate of the temperature change decreased to slowly reach the steady-state regime. Thermal gradient through the section depth was also developed in a way that severe temperature gradients (as large as 150 °C) were observed in the lower portion of the exposed cross section, while small differences (≤ 17 °C) were exhibited in the temperatures of the upper portion.

Figure 3 shows the temperature distribution (at 11 different sections shown in Figure 1) along the specimen length before the fire was extinguished. Temperatures in this figure were the average values of tc readings from the repeated tests, with the expanded uncertainty (± *U*) indicated as error bars. *U* was estimated based on the estimated values of the standard[‡] (u_c) with a coverage factor of 2 (95% confidence interval). As shown in the figure, the thermal gradient along the beam length developed under two different fire conditions were similar. The constant HRR tests (Tests 3 through 5) showed a better representation of the symmetric thermal gradient with respect to the centerline of the beam specimen than the other tests (Tests 1 and 2).

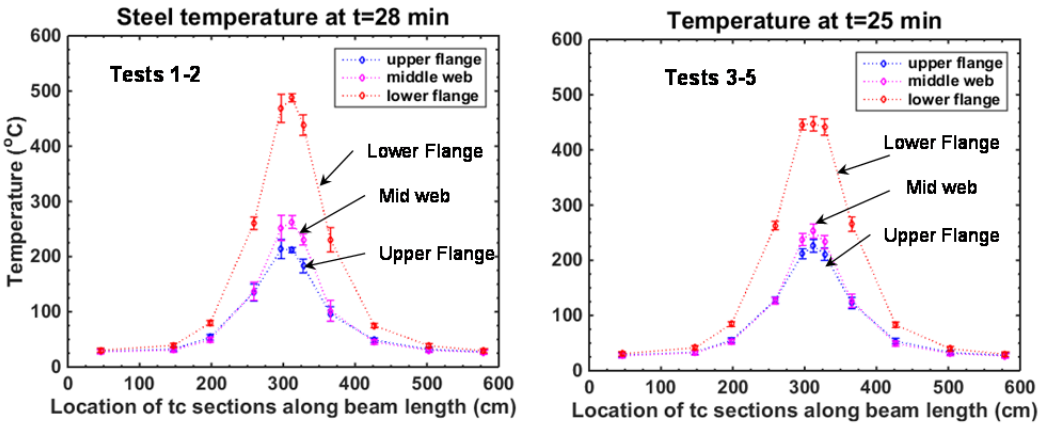


Figure 3. Thermal gradient along the beam length

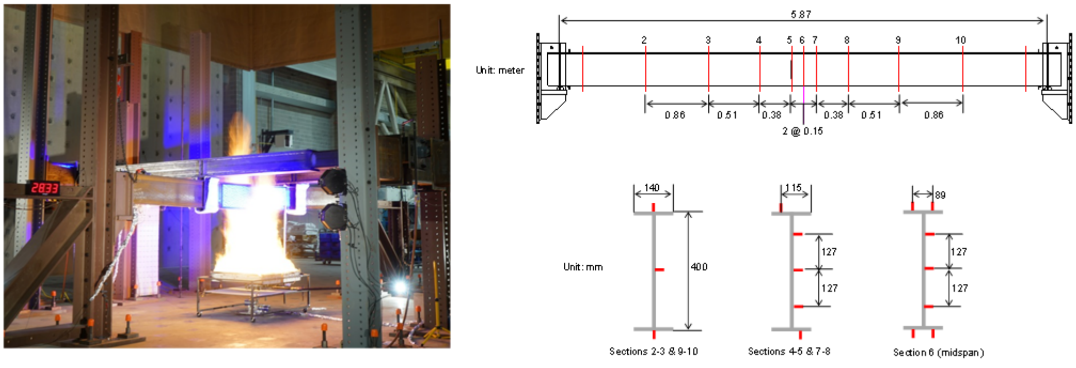
[‡] The components of standard uncertainty (u_c) included test repeatability estimated using uniform distribution and manufactures' specifications on thermocouple error (± 0.4%) and digitization error (± 3.2 ˚C) with 95 % confidence interval. Test repeatability was estimated using individual data points at specific tc locations (Figure 1) at a specific time of occurrence (t) after ignition. For sections 4 through 8 (Figure 1), there were two thermocouples at the upper and lower flanges each. These two tc readings were averaged to represent the upper and lower flange temperate at the specific location of the section.

STRUCTURAL FIRE TEST

Test setup, test protocol, and instrumentation layout

The W16×26 steel beam specimen was tested under combined flexural loading and a localized fire condition. Figure 4 shows the structural fire test setup. The same natural gas burner used in the fire-thermal tests was used to create a localized, open flame fire exposure directly to the critical sections (i.e., expected plastic hinge zone) of the specimen. For the structural loading, two hollow steel section (HSS) loading beams (placed on the top of the specimen) served as two point loads to produce a uniform bending moment across the fire-exposed critical sections of the beam specimen. The distance between the two loading points was 2.44 m (8 ft). The ends of the two HSS loading beams were connected to four 235 kN (53 kip) actuators via four 34.9 mm (1.38 inch) diameter high-strength steel rods. The high-strength steel rods had no rotational restraints at the ends. The actuators were mounted to the underside of the strong floor to protect them from fire. The HSS loading beams were water-cooled during the fire exposure.

The beam specimen was simply supported such that both end rotations about the principal axes and the axial (longitudinal) displacements were not restrained, whereas the beam ends were laterally restrained. The bearing-to-bearing length of the specimen was 5.87 m (19.25 ft). The room-temperature yield and ultimate strengths of the specimen were (440 ± 1.15) MPa and (530 ± 1.73) MPa, respectively[§].



Thermocouple layout

Figure 4. Structural fire test setup and thermocouple layout

The test was conducted in two steps as follows: (i) The HRR of the burner was increased to a target magnitude of 700 kW and maintained constant throughout the test. (ii) After the maximum temperature at the fire-exposed cross sections reached the steady-state condition, two point loads were programed to increase at a rate of 2 kip/min (8.90 kN/min) simultaneously until the failure occurred.

For temperature measurements, a total of thirty nine, type-K, 24 gauge thermocouples were installed at nine different cross sections along the beam length as shown in Figure 4. Four plate thermometers and a thermal imaging camera were installed to supplement the temperature data of the specimen. The vertical and lateral

[§] The standard uncertainty (u_c) is estimated based on the certified material test report provided by steel fabricator and the assumption of uniform distribution. The numbers following the symbol ± are the expanded uncertainty (U) with a level of confidence of approximately 95%.

displacements of the beam specimen in the fire-exposed zone were measured using specially designed potentiometers with temperature compensation. Two rotational transducers were installed at the specimen ends to measure the rotations about the principal axes of the beam cross section. The digital image correlation method was also used to measure the three-dimensional strains in the fire-exposed zone of the specimen. Technical details of the high-temperature displacement and strain measurements were not presented in this paper for brevity and because they are still under development. In addition to four actuators to apply and measure the structural loads, a 222 kN (50 kip) load cell were installed at each end of the beam specimen to measure the reaction forces during the test.

Test results

Figure 5 shows the test results including (i) the HRR data from the burner, (ii) the temperature data at the critical section (i.e., expected plastic hinge zone) of the specimen, (iii) the applied bending moment data, and (iv) the vertical displacement data at the fire-exposed midspan of the specimen. Note that the temperature data in Figure 5 are the average values of thermocouple readings of sections 5 and 6 only (Figure 4) and those of section 7 are not included as a result of flame lean during the test. The failed section was also located between the sections 5 and 6.

With the HRR-time relationship shown in Figure 5, the lower flange temperature reached steady-state at approximately 21 min. While the HRR of the burner was increased to 700 kW, no structural load was applied other than the self-weight of the specimen and the two water-filled HSS loading beam assemblies (16.7 ± 0.4 kN). The thermal gradient was developed through the cross sections, which resulted the thermal bowing about the strong axis.

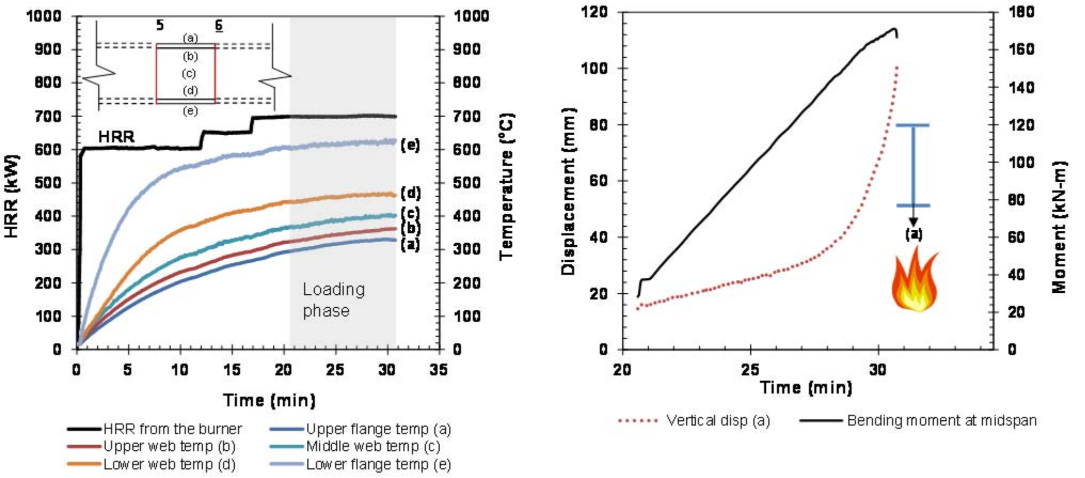


Figure 5. Fire-temperature and structural behavior of the beam specimen.**

** The temperature data has a maximum expanded uncertainty (*U*) of 34.0 ˚C calculated from a combined standard uncertainty (u_c) of 17.0 ˚C and a coverage factor of 2 (95 % confidence interval); The bending moment has *U* of 10.4 kN-m calculated from u_c of 5.2 kN-m and a coverage factor of 2. The vertical displacement data has *U* of 0.3 mm with a coverage factor of 2.

Under the loading phase where the HRR from the burner was maintained at a set point of 700 kW, the bending moment was applied at a rate of (14.7 ± 0.3) kN-m/min until failure occurred at approximately 31 min. The maximum temperature (at the lower flange at midspan) was (642 ± 28) ˚C, while the HRR was maintained at 700 kW. As shown in Figure 5, the vertical (downward) displacement of the beam specimen linearly increased with linearly increasing bending moments until the moment reached 124 kN-m (39 % of the plastic moment capacity at ambient temperature calculated using the plastic modulus in the steel manual [3]), then the nonlinear behavior was followed until failure. The increase in lateral displacements at midspan was also initiated at 124 kN-m. The measured peak moment capacity was 171 kN-m (54 % of the plastic moment capacity at ambient temperature) followed by runaway displacements. The failure was indicated by a sudden drop of the reaction force accompanied with rapidly increasing (runaway) displacements. As soon as the applied load and fire was removed, the beam specimen slightly bounced upward.

Figure 6 shows the photographs of the specimen at failure and the deformed shape of the specimen after cooling. Overall, when subjected to increasing flexural loads and the 700 kW fire, the beam specimen behaved in a complicated way that flexural bending and lateral torsional behavior were exhibited simultaneously.

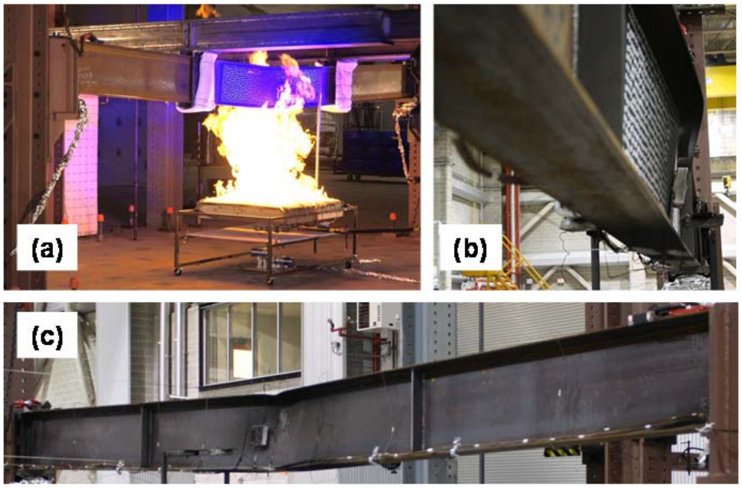


Figure 6. Photographs of (a) the beam specimen at failure, (b) the lateral-torsional deformation at the fire-exposed region, and (c) the beam specimen after cooling down.

SUMMARY

The open flame, localized fire tests were conducted on 6.17 m long W16×26 beams with simply supported boundary conditions. The experimental tests consisted of two parts: (1) fire-thermal tests to evaluate the effects of the prescribed heat release rates (HRR), provided by the 1 m × 1 m natural gas burner, on the thermal responses of the steel beam specimen and (2) structural-fire test to evaluate the effects of the localized fire on the behavior and the load-bearing capacity of the steel beam specimen. The cross sections at midspan (i.e., expected plastic hinge zone) of the beam specimen were directly exposed to a natural gas fire.

The test results indicated that the prescribed heat release rates from the burner affected the heating rate of the steel beam specimen. When the HRR-time relationship of the burner followed the step function with 100 kW increments approximately every 5 minutes, the temperatures at the fire-exposed region of the beam specimen increased linearly with increasing fire exposure time. When the HRR was set to a constant target magnitude of 400 kW, the specimen temperature indicated nonlinear heating to reach the steady-state condition. When the beam specimen was subjected to linearly increasing flexural loads at maintained HRR of 700 kW, combined flexural and lateral torsional failure of the specimen was exhibited. The peak moment capacity was achieved at 171 kN-m, which is 54 % of the plastic moment capacity at room temperature.

The test results from the present study can be used for developing or calibrating analytical models, which can be eventually used for evaluating the performance of structural members subjected to a localized fire. The findings from this study are limited to the range of parameters included in the tests. Further evaluation on the effects of various boundary conditions (axial and rotational restraints) and heating rates on the fire performance of the beam specimens are currently on going.

ACKNOWEDGEMENT

The research presented in this paper was carried out under the NFRL Infrastructure and Commissioning project which seeks to deliver a fully operational NFRL, including outfitting of laboratory infrastructure and verifying operation and calibration of individual and combined fire and structural systems. We thank our colleagues Matthew Bundy, Anthony Chakalis, Artur Chernovsky, Leaurean DeLauter, Matthew Hoehler, Doris Rinehart, Brian Story, Christopher Smith, Nelson Bryner, and Jian Jiang who provided insight and expertise that greatly assisted the experimental research at NFRL or helped to improve the paper.

REFERENCES

1. Bundy, M., Hamins, A., Gross, J., Grosshandler W., Choe, L. 2016. "Structural Fire Experimental Capabilities at the NIST National Fire Research Laboratory," *Fire Technology.,* pp. 1-8, doi:10.1007/s10694-015-0544-4.
2. ASTM International. 2015. "Standard Specification for Structural Shapes," Standard A992, ASTM International, W. Conshohocken, Pa.
3. AISC. 2010. Steel Construction Manual, 14th edition, American Institute of Steel Construction (AISC), Table 1-1, Chicago, IL
4. Bryant, R., Bundy, M., Zong, R. 2015. "Evaluating Measurements of Carbon Dioxide Emissions Using a Precision Source—A Natural Gas Burner," *J. the Air & Waste Management Association*, 65(7), pp, 863-870. doi: 10.1080/10962247.2015.1031294.

Adaptive Multi-scale PHM for Robotic Assembly Processes

Benjamin Y. Choo[1], Peter A. Beling[2], Amy E. LaViers[3], Jeremy A. Marvel[4], and Brian A. Weiss[5],

[1,2,3] *University of Virginia, Charlottesville, Virginia, 22904, USA*

byc6j@virginia.edu
beling@virginia.edu
alaviers@virginia.edu

[4,5]*National Institute of Standards and Technology, Gaithersburg, Maryland, 20899, USA*

jeremy.marvel@nist.gov
brian.weiss@nist.gov

ABSTRACT

Adaptive multiscale prognostics and health management (AM-PHM) is a methodology designed to support PHM in smart manufacturing systems. As a rule, PHM information is not used in high-level decision-making in manufacturing systems. AM-PHM leverages and integrates component-level PHM information with hierarchical relationships across the component, machine, work cell, and production line levels in a manufacturing system. The AM-PHM methodology enables the creation of actionable prognostic and diagnostic intelligence up and down the manufacturing process hierarchy. Decisions are made with the knowledge of the current and projected health state of the system at decision points along the nodes of the hierarchical structure. A description of the AM-PHM methodology with a simulated canonical robotic assembly process is presented.

1. INTRODUCTION

Prognostics and Health Management (PHM) refers to a class of techniques and methods that enable condition monitoring of a physical machine or functional process. PHM encompasses health monitoring of a system; provides diagnostic information including what is at fault, why the fault occurred, and how the fault can be remedied; and offers prognostic intelligence as to when a system or process is going to degrade to various states that may include going out of specification or failure.

A manufacturing system is a complex system-of-systems with a hierarchical structure. A manufacturing system hierarchical structure is described as a facility consisting of multiple assembly/fabrication lines that are further divided into work cells or work stations which are further divided into multiple machines consisting of components (Hopp & Spearman, 2008). One challenge in PHM for manufacturing is that in most applications data gathering and analysis is limited to the component level. For example, prognostic intelligence for machines, such as robots or machine tools, typically does not propagate beyond the boundaries of the machine even though the failure of a single component may lead to failure of other components or to system-wide effects.

The use of PHM technologies in manufacturing operations continues to experience growth driven by advances in sensor, computing, and communications technologies, and in machine learning and other data analytic techniques. An increased interest in PHM within manufacturing is also reflected in recent academic literature. Yoon, He, and Van Hecke (2014) applied PHM to an additive manufacturing process for improved fault diagnosis and quality control. Philippot, Marang, Gellot, Ptin, and Riera (2014) suggest a fault tolerant control structure for manufacturing plant control. The self-aware machine platform for application in a manufacturing shop floor proposed by Liao, Minhas, Rangarajan, Kurtoglu, and de Kleer (2014) provides a richer set of PHM information, including predicted component wear and real-time anomaly detection to the shop supervisor. However, there is a notable absence of methodologies to support the development of agile and flexible PHM systems in smart manufacturing environments (Peng, Dong, & Zuo, 2010).

Ideally, PHM would be available at the system level, including prognostic intelligence being propagated up the hierarchical structures that relate components to machines, machines to work cells, and work cells to production lines. Model-based diagnostic methods that have been developed for hierarchical aerospace systems may be applied to hierarchical manufacturing systems. For example, Narasimhan and Brownston (2007) suggested a general

Benjamin Choo et al. This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 United States License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

framework for stochastic and hybrid model-based diagnostics for aerospace systems. Feldman, de Castro and van Gemund (2013) proposed a decision support framework for satellite systems that uses active testing to increase diagnostic accuracy. Biswas and Mahadevan (2007) also proposed a framework for system health management that includes fault detection, fault identification, and adaptive control for aerospace applications. In the manufacturing domain, Celik, Lee, Vasudevan, and Son (2010) applied a dynamic data-driven framework on a supply chain system to perform multi-fidelity simulation. Ferri, Rodrigues, Gomes, de Medeiros, Galvo, and Nascimento (2013) have suggested a method for achieving system-level PHM by propagating the remaining useable life (RUL) along the fault tree structure of the manufacturing system model. This is a positive step in creating a methodology for achieving system-level PHM within Smart Manufacturing based on the system model and component-level PHM.

To address the existing gap in providing PHM for hierarchical manufacturing systems, we propose a methodology termed Adaptive Multiscale PHM (AM-PHM). The AM-PHM methodology is designed to support PHM in Smart Manufacturing Systems (SMS). AM-PHM is characterized by its incorporation of multi-level, hierarchical relationships and PHM information gathered from a manufacturing system. AM-PHM utilizes diagnostic and prognostic information regarding the current health of the system and constituent components, and propagates it up the hierarchical structure. By doing so, the AM-PHM methodology creates actionable prognostic and diagnostic intelligence along the manufacturing process hierarchy. This information includes the predicted health state upon completion of a task. The AM-PHM methodology allows for more intelligent decision-making to increase efficiency, performance, safety, reliability, and maintainability.

AM-PHM, at a given level along the system hierarchy, uses operational profiles from adjacent, higher-level operational profiles. These profiles describe the production goals under consideration by the decision-makers (e.g., operators and supervisors) at the higher level. In addition to the traditional workload, bill of materials, and requirements of the manufacturing process, the operational profile may have a focused objective such as minimizing cost or maximizing reliability. One instantiation of the AM-PHM concept may be as an AM-PHM module situated at every node along the hierarchical structure. The AM-PHM module gathers PHM information from subordinate systems or components and makes a decision ideal for the task corresponding to the operational profile. The AM-PHM module then creates operational profiles for its subordinate AM-PHM modules while producing diagnostic and prognostic information for its higher-level subsystem.

An example robotic assembly process is selected to show the effectiveness of the AM-PHM methodology. In today's manufacturing world, the finished products/goods are becoming more complex as machines with increased capabilities are being deployed to the manufacturing floor. One example is the utilization of the industrial robot.

Worldwide, the manufacturing landscape has experienced extensive growth in the development and deployment of new robotic technologies. Paired with the introduction of newer, cheaper, and more reliable sensing technologies, the capabilities of robotic systems have improved in a relatively short amount of time. Processes that were historically performed by manual labor may now be accomplished using robots. As such, the use of robots outside of the automotive and electronics industries is on the rise (Orcutt, 2014).

Global manufacturing initiatives are stressing the development and integration of smart manufacturing technologies in modernized manufacturing facilities. Such technologies are seen as key to maintaining economic stability within an increasingly competitive global market (Holdren et al, 2011).

Robotic assembly is expected to be a principle application of robotics in manufacturing (Marvel & Falco, 2012). Historically, mechanical assembly has been addressed by manual labor. However, advancements in robotic perception, force control, and kinematic dexterity have enabled robotics to be viable options for assembly applications. This expands the traditional application suite of material handling, painting, and welding that have been more typical of robotic operations in manufacturing. Moreover, with the introduction of collaborative robot technologies, the expansion of robotics is expected to positively impact manufacturing processes that remain largely manual in nature (Marvel, 2014).

With the anticipated integration of robots into both new and preexisting manufacturing lines, the quality of PHM will directly influence the effectiveness of interoperability and system performance. This is particularly true when humans are expected to work alongside robotic collaborators, where robot performance also impacts safety. Should a robotic system experience a failure, it is expected to do so in a safe, reliable manner that does not negatively impact its environment, process, or collaborators. Moreover, the road to recovery must be clearly established and easy to implement. This necessitates significant advancements in the quality and dissemination of robotic PHM.

The remainder of the paper is organized as follows. Section 2 examines the current state of PHM capabilities and standards in manufacturing. Section 3 presents the AM-PHM methodology including the proposed AM-PHM features for describing the health state of systems. Section 4 discusses two example implementations of the AM-PHM methodology as applied to a test robotic assembly production line scenario. Section 5 concludes the paper by highlighting the significance of AM-PHM in manufacturing.

2. Current State of PHM in Smart Manufacturing

PHM technologies in manufacturing systems reduce time and costs for maintenance of products or processes through efficient and cost-effective diagnostic and prognostic activities. In 2010, a comprehensive review was conducted of prognostic and diagnostic methodologies for condition-based maintenance (CBM) that presented the existing strategies within four categories: physical models, knowledge-based models, data driven models, and combination (hybrid) models (Peng et al., 2010). This review highlighted many specific methods across four categories (Hidden Markov Models, Bayesian network-related methods, Fuzzy Logic, Principal Components Analysis) along with their successes and limitations. No method stood out as being sufficient to provide both diagnostic and prognostic intelligence at multiple levels. This review demonstrated that for every method's strength, there was at least a single weakness. Similarly, another review of existing methods for manufacturing systems was conducted in 2012 that focused on comparing time-based maintenance (TBM) and condition-based maintenance (CBM) (Ahmad & Kamaruddin, 2012). TBM, commonly referred to as preventative maintenance, is typically simpler to implement (in that maintenance is scheduled based upon a specific unit of time; e.g., cycle time) while CBM, sometimes termed predictive maintenance, may ultimately be more cost effective if a process's or equipment's health data accurately reflects its current state and allows a machine to run longer until maintenance (as compared to a TBM schedule). The challenge in CBM is gathering sufficient data to make a reasonably accurate prediction.

Product PHM (providing health monitoring, diagnostics, and/or prognostics for a finished system; e.g., automobile, aircraft, power generation station) is more widespread as compared to process PHM (providing health monitoring, diagnostics, and/or prognostics to a system that integrates one or more pieces of equipment to complete a task; e.g., assembly process, welding process, machining process) (Batzel & Swanson, 2009) (Holland Barajas, Salman, & Zhang, 2010) (Hu & Koren, 1997) (Shen, Wan, Cui, & Song, 2010). Likewise, PHM techniques have been developed and applied more widely at component/ equipment levels, yet some work has occurred at the higher/ system levels. For example, innovative methods have been developed to support various machining operations (Al-Habaibeh & Gindy, 2000) (Altintas, Verl, Brecher, Uriarte, & Pritschow, 2011) (Biehl, Staufenbiel, Recknagel, Denkena, & Bertram, 2012) (Borisov , Fletcher, Longstaff, & Myers, 2013). System-level PHM methods have also been developed, yet seem to be focused in their applicability and/or limited in capability (Barajas & Srinivasa, 2008) (Datta, Jize, Maclise, & Goggin, 2004) (Hofmeister, Wagoner, & Goodman, 2013).

Vogl et al. (2014) conducted a detailed review of existing standards that were designed to help guide implementation of PHM in manufacturing. Specifically, many of the current PHM standards were developed within the International Organization for Standardization (ISO) and focus primarily on condition monitoring and diagnostics (ISO, 2002) (ISO, 2003) (ISO, 2012). Few standards include discussion of prognostics (ISO, 2004). Most standards fall into one of two categories; standards that are very specific and only applicable to a few processes and standards that are very broad that may lack guidance for applications. Likewise, no standard has been developed that offers the flexibility to be applied at multiple hierarchical levels of a complex system to promote effective PHM practices.

3. Adaptive Multiscale PHM for Smart Manufacturing

A manufacturing system hierarchical structure can be described as a facility consisting of multiple assembly/fabrication lines which are further divided into work cells or work stations which are further divided into multiple machines (Hopp & Spearman, 2008). For this paper, the hierarchical structure of the facility, assembly line, work cell, and machine will be used as a primary example, although there exists more complex methods of describing a manufacturing facility.

Information is passed down in the form of orders, schedules, bills of materials, or control signals between each hierarchical level of the system. The job of the subordinate system is to follow the tasks assigned by the higher-level node. Historically, maintenance policies for machines have been based on usage time or workload, as static policies defined in these terms can be estimated through historical data and experience. An effort to modify this approach into a feedback system where the health state of the machine or component is considered in making maintenance decisions emerged only recently. (National Institute of Standards and Technology, 2015) However, health state information is often confined to the component or machine level and is not propagated up to the system level.

On the other end of the spectrum, the system-level approach to analyzing a manufacturing system has resulted in generalized risk and fault analysis methods such as fault tree analysis (FTA) and failure mode and effects analysis (FMEA) (SAE International, 2009). Also, modeling software tools such as SysML have been used to describe the system structure including interoperability and interdependency between components of the system (Wünsch, Lüder, & Heinze, 2010).

The AM-PHM methodology is designed to provide decision-makers with enhanced information on the current and predicted health state of the decision-maker's subsystems. Figure 1 depicts the AM-PHM methodology for a simple hierarchical manufacturing structure.

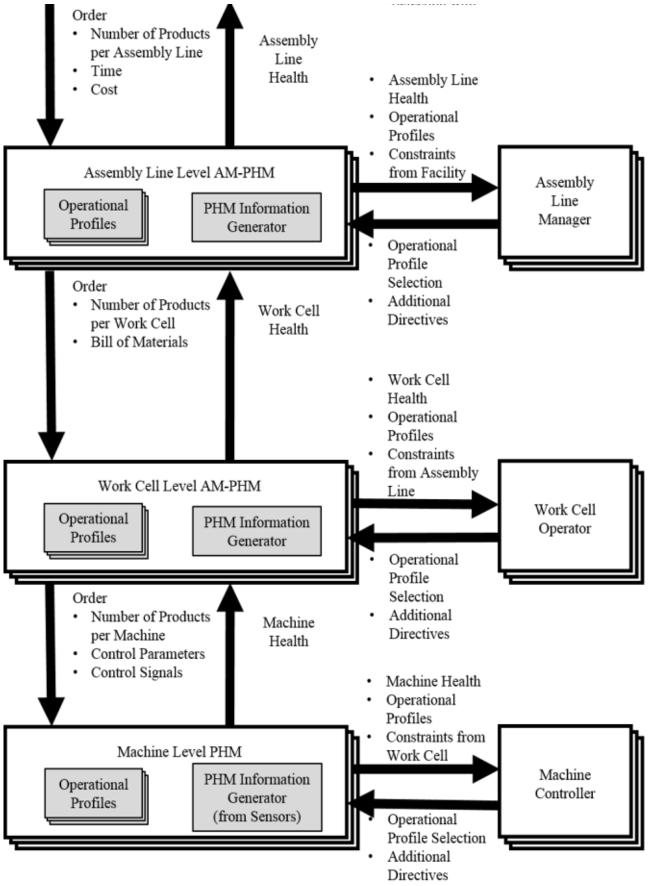


Figure 1. Conceptual representation of AM-PHM

For AM-PHM, a decision-maker is not limited to the machine operator. Rather, it refers to any person or machine such as the control unit of a manufacturing robot or the supervisor of an assembly line that is responsible for making decisions that can influence the outcome of the system. The point at which the decision-maker resides in the hierarchical structure is called the decision point within the AM-PHM methodology. Conceptually, an AM-PHM module resides at every decision point of the hierarchical structure of the manufacturing system.

A hierarchical manufacturing system refers to a manufacturing system in which multiple levels exist. For each level, the higher-level nodes encompass the lower-level nodes. In this level structure, the parent nodes have control over the states of its subsystems while subsystems do not have direct control over the states of its parent nodes. Examples of the hierarchical structure may be a SysML description or a fault tree structure of the manufacturing system. Another example may be a treelike description of the physical setup of a manufacturing system consisting of assembly lines, work cells, and machines.

For the example structure shown in Figure 1, an order is placed to the Facility Manager with the number of products requested, product requirements, and expected finish date. The order information and the operational directive are passed onto the facility level AM-PHM module. The directive refers to a particular set of attributes or objectives that the decision-maker would like to focus on. For example, the decision-maker may be interested in reducing the time, cost, risk, or wear in maximizing the utilization rate.

The facility level AM-PHM module reports the health information of the facility to the Facility Manager. PHM information on the subsystem is needed for effective directive-driven decisions to be made. The PHM information from the subsystem is processed at each AM-PHM module. This results in health metrics that appropriately represent the current and future state of the system. These health metrics may include remaining usable life of the system, expected health state upon completion, nature of fault, and proposed solutions.

The AM-PHM module also creates operational profiles once all aforementioned information is gathered. Each operational profile is designed to control the subsystems with a focused directive. The operational profile also contains the projected health information for the subordinate systems such as projected health upon completion. The decision-maker may now choose from the set of operational profiles that fit within the constraints handed down from its superior nodes.

The Facility Manager selects the operational profile that best fits the directive and order requirements. Once the operational profile is chosen, the set of instructions contained within that operational profile are handed down to the subordinate AM-PHM module and a similar process repeats itself. For the example in Figure 1, the selected operational profile containing the number of products needed to be produced by each production line and operational directive is passed down to the Assembly Line level.

A similar process is now repeated at the Assembly Line level. The Assembly Line Manager takes the operational profile handed down from the Facility level and selects an appropriate operational profile. The operational profile handed down to the Work Cell level contains information such as number of products produced for a particular work cell and bill of materials needed for the processing of the order.

A similar process is repeated for the Machine level. For the Machine level the operational profile contains machine operation parameters and the AM-PHM information contain data such as the aggregated wear for critical components.

Although the simplified scenario depicted in Figure 1 is convenient for initial discussion of the AM-PHM concept, the concept may be expanded for more general SMS environments in which there exists an extensive hierarchy of processes and components.

Additional features that better describe the current health state at a particular juncture of the system are needed for the AM-PHM system to be helpful to the decision-maker. The newly suggested features are (a) *greatest wear*, (b) *average wear*, (c) *health balance score*, (d) *probability of successful completion*, and (e) *estimated health state upon completion*.

(a) *Greatest wear* represents the most extreme wear in percent from all the wear states of all the subordinate components. This gives an idea of the state of the most worn component of the system.

(b) *Average wear* represents the arithmetic weighted mean of the wear in percentage of all the subordinate components. This metric represents the overall average health state of the system. The average on its own may not reveal much information but in conjunction with the *greatest wear* and the *health balance score*, this helps to describe the health state of the all the components of the subsystem. Different components contribute differently to the overall performance of a manufacturing system. There are established methods such as FTA, FMEA, Hierarchical Holographic Modeling (HHM), and Risk Filtering, Ranking, and Management (RFRM) that may be used to analyze the weight of each component to different failures. The differing importance of a component is included as a weighted coefficient.

(c) *Health balance score* is the standard deviation of the wear state of each of the subordinate components at a given node. This metric indicates degree of concentration of wear of the system. A higher number would indicate that wear values vary greatly among components, while a smaller number would indicate that the system has similar wear along most of its components.

(d) *Probability of successful completion* is the probability that the component will complete the given operational profile with the current state of health. This gives decision-makers an idea of the success rate or confidence involved with a given solution.

(e) *Estimated health state upon completion* refers to the expected final state of health for all metrics involved in AM-PHM. This is used to show a predicted picture of the overall state of health at the point of completion of the assigned task.

The *average wear, health balance score*, and *probability of successful completion* may be further customized so that each of the components carry different weights. This means the proposed metrics can focus on certain components depending on its importance within the overall structure of the system.

One notable point for the proposed features is that the basis for the usefulness of these metrics lies on the assumption that the PHM information from the component level is accurate to a certain degree. An accurate wear model is necessary for the health metrics to be useful.

4. AM-PHM Implementation in Smart Manufacturing Robotic Assembly

An example assembly line involving multiple robots is described in this section. The AM-PHM methodology is applied to the canonical manufacturing process simulation. The canonical process is a generalized test case of the example assembly line and includes related assumptions. This simplified test case, including its simulated results, highlights the usefulness of the AM-PHM implementation. The structure and the trend of the numbers involved are reasonable in real manufacturing settings. The use of robotic arms in industry is widespread as stated in Snyder (1985) and the trend of the drill wear in the canonical example simulation follow the model by Kadirgama, Abou-El-Hossein, Noor, Sharma and Mohammad (2011).

The example hierarchical structure of a manufacturing environment consists of a single assembly line with multiple work cells, each of which has multiple machines, each comprised of multiple components. The operational profiles flow from the higher-level block to the lower-level blocks in the AM-PHM framework. The PHM information is reported from the lower-level blocks up to the higher-level block. However, both the operational profile and the PHM information are processed appropriately for each level.

The specific information that is listed in the operational profiles and the PHM reports differ depending on the block's location in the hierarchical structure. For example the operational profile generated by the assembly line for each work cell will resemble a bill of materials; the operational profile generated by the work cell for each machine will resemble a process instruction; and the operational profile generated by the machine to its components will be close to a set of control signals.

The operational profile generator of the AM-PHM module at each level must translate the task it receives from the higher-level AM-PHM module into a task that can be understood by the subordinate level. Similar concepts apply to the PHM information at each stage. The PHM information from the component to the machine will include RUL of replaceable parts, while the PHM information from the machine to the work cell includes more information on the tradeoffs involved with different operational profiles. Finally, the PHM report from the work cell to the assembly line would include more information on the probability of successful completion and the overall health state of the work cell. The AM-PHM module must process the PHM information it receives from the lower levels and provide value-added, level appropriate information for the upper level.

Two different examples of AM-PHM are given. The first example is focused on a simple AM-PHM structure with simple operational profiles and a PHM report involving only RUL. This structure may be implemented if the nature of the task performed at an assembly line does not require sophisticated PHM capabilities or if changing the existing system model and fault tree structure is not desired. The deployment of AM-PHM into the existing assembly line model is minimally invasive and most likely will not affect the overall structure of the fault tree.

The second example is a more sophisticated AM-PHM system. This is needed if the assembly line handles a more complex process involving many different machines with interdependencies and interoperability. The downside is that the implementation may become more complicated and the use of AM-PHM may impact the existing fault tree structure of the system model.

In the canonical example, a robot with two drilling arms is used to drill holes into a box. The left and right drilling arm are each responsible for drilling holes into the left and right side of the box, respectively. A SysML model of the drilling robot is presented in Figure 2. The corresponding FTA diagram of the drilling robot is shown in Figure 3. Only the flank wear of the drill bit component on each arm is considered for the simplified AM-PHM example, as flank wear is one of the common wears exhibited in drilling (Kadirgama et al. 2011). It is important to note that one drilling arm may perform the job of the other drilling arm with the penalty of reduced production rate.

In real-world manufacturing systems, there are many factors such as material properties, work piece structure, and machine characteristics that are carefully considered when selecting machining parameters. Machining parameters are optimized to best fit the particular manufacturing process. However, in a complex system-of-systems, optimization based on one feature means there is a trade-off with other features. Also, for a particular process there is a range of acceptable machining parameters rather than one fixed operating point (Furness, Wu, and Ulsoy, 1996). Drill bit manufacturers recommend a range of feed rates and cutting speeds for their drill bits (Sandvik Coromant, 2005).

When the parameters for a process are selected, the model [for the process] does not account for the fact that the system may change as the machine experiences wear in its components. The wear of the components, such as the flank wear of the drill bit, affects the characteristics of the system. Thus, the optimal operating parameters may need adjustment to account for the change in the system caused by the deteriorating health state of the machine.

For the canonical process example simulation, simplifications are made to emphasize the effect of the AM-PHM methodology and to reduce the complexity of the example. The drilling robot is tasked to drill 100 holes on the left and right side of the box. The left and right drilling arm each drill on their respective sides, simultaneously. Though there are several different types of wear involved with the drill bit, only the flank wear occurring on the cutting edge of the drill bit is considered.

The work piece is made of Nickel alloy with a Brinell hardness of 200. The production line has identified an acceptable and stable range of operating parameters. The cutting speed is between 100 m/min to 180 m/min. The feed rate is between 0.1 mm/rot and 0.2 mm/rot. Each hole has a cutting depth of 1.5 mm and the drill diameter is 10 mm. Expected tool life is different for different combinations of cutting speed and feed rate and follows the values stated by Kadirgama et al. (2011).

The drill bit is considered completely worn and reached its replacement point when there is 0.3 mm of flank wear. The RUL or tool life depends on the machining parameters and the replacement threshold for the drill bit. Tool life also differs depending on the size and geometry of the drill bit. Thus, to provide a more comparable quantitative figure for the amount of wear, the wear is presented as a percentage. The wear percentage is calculated by dividing the remaining tool life by the tool life for a new tool.

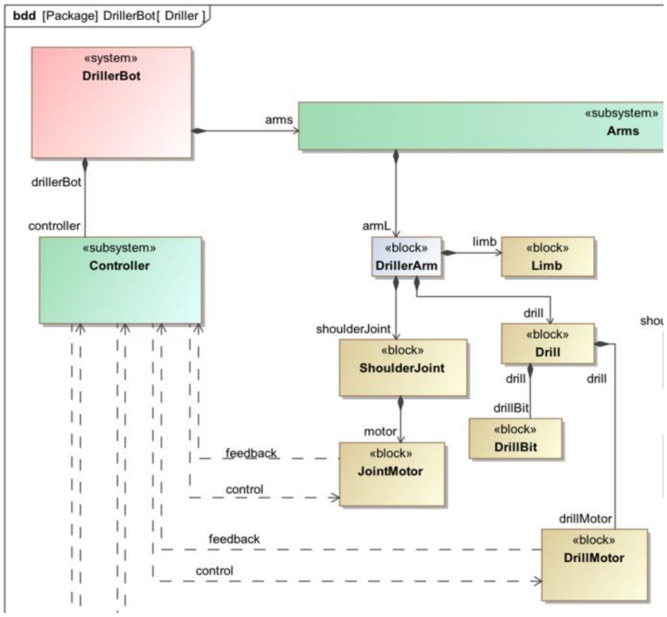


Figure 2. SysML description of drilling robot

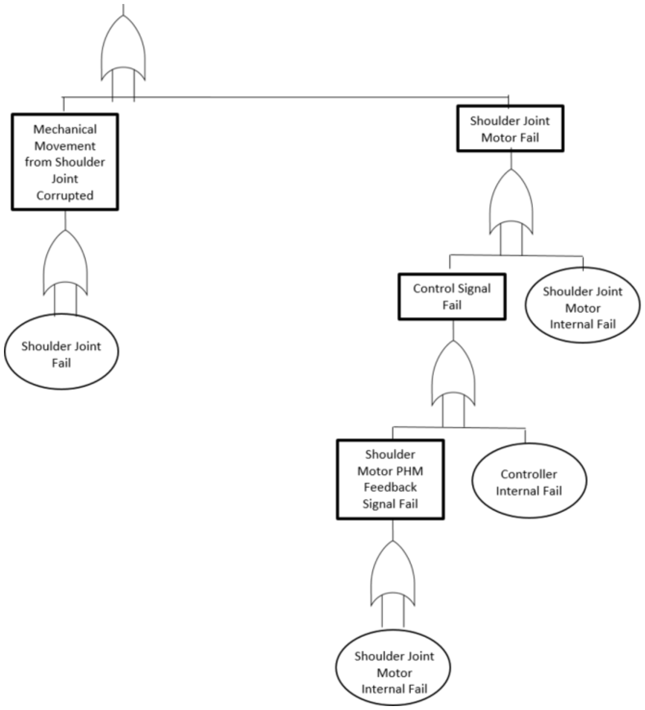

Mechanical Movement from Shoulder Joint Corrupted
Shoulder Joint Motor Fail
Shoulder Joint Fail
Control Signal Fail
Shoulder Joint Motor Internal Fail
Shoulder Motor PHM Feedback Signal Fail
Controller Internal Fail
Shoulder Joint Motor Internal Fail

Figure 3. Fault tree analysis (FTA) of drilling robot

4.1. Simple Implementation of AM-PHM

The AM-PHM module is implemented on the canonical example robotic assembly process. Only the RUL is propagated based on the system's SysML model to provide RUL information along the system's hierarchical structure.

Two methods by Mhenni et al. (2014) and Ferri et al. (2013) were combined to achieve this task. Mhenni et al. (2014) suggested a method for converting a SysML model into a fault tree. The method uses templates that translate several basic SysML subcomponent blocks into an equivalent fault tree structure. Then rules are suggested for combining these small fault trees into a complete system fault tree. Figure 3 shows the fault tree constructed using this automated algorithm. The leaf nodes of the fault tree correspond to the individual components of the left arm of the driller robot.

Another example PHM technique that could be applied within AM-PHM was developed by Ferri et al. (2013). This research team developed a method for propagating the RUL along a fault tree. This methodology takes the RUL of the end components and applies a set of rules to produce the RUL at each node of the fault tree. The PHM capability provides the RUL for each component. The individual component-level RUL is combined, resulting in the overall RUL for the driller robot.

A semi-automated method for building system-level AM-PHM is completed through the combination of these two methods. The system-level RUL is produced given the availability of the SysML model and component-level RUL. In this case, the actual implementation of the AM-PHM is done through the use of FTA as an intermediate, semi-automated step of linking system-level hierarchical information and component-level health information. Only the RUL given at each level is used as the source of health information.

The work cell is tasked to build 20 boxes. The starting wear state of the individual drill bits are 85 % worn for the left drill in Robot 1 and new for all other drill arms. The default operating speed is set to a feed rate of 0.2 mm/rot and 120 m/min. This results in a wear rate of 15 % per minute for the drill bit and a production rate of 5 boxes per minute. The component-level RUL is calculated based on this initial condition. The component-level RULs show that for Robot 1, the left arm has an RUL of 1 minute and the right arm has an RUL of 6.6 min. For Robot 2, both the left and right arm has an RUL of 6.6 min. This information is propagated along the hierarchical structure according to the rules. Robots 1 and 2 each result in RULs of 1 minute and 6.6 min, respectively. The decision to distribute the load to the two robots is made based on the production targets and RUL information by the work cell operator. A work load of five boxes is assigned to Robot 1 and a work load of 15 boxes is assigned to Robot 2. The job takes three min to complete and the final RUL upon completion for each robot is 0 and 3.6 min, respectively. The complete results including additional information on the health of the work cell are presented in Table 1.

The result shows that the system has an RUL of 3.6 min. This is information previously unattainable to the decision-maker. Utilization of the RUL information enables more efficient use of the components of the manufacturing system. The advantage of this degree of PHM reflection is that at any point in the hierarchical structure the same RUL calculation method can be applied again reducing the complexity of implementation. The upper-level RUL is calculated using simple multiplication and comparison process. This begins by converting the fault tree (consisting of logic AND and OR gates) to a sum of products (SOP) expression. Once the SOP expression for the system is obtained, the system RUL is calculated by multiplying the probability distribution of the RULs for the product terms of the expression. The next step is to select the appropriate RUL for the sum portion of the expression. The system RUL ends up highlighting the set of components that are contributing to the nearest expected system failure. However, the system RUL does not contain health information on the other components of the system that are not directly tied to the upcoming failure. This limits the range of intelligent decisions that can be made.

Table 1. AM-PHM based manufacturing results using RUL

Time (min)	0	1	2	3
Production Rate of Robot 1 (box/min)	5	5	-	-
RUL of Robot 1 (min)	1	0	-	-
Production Rate of Robot 2 (box/min)	5	5	5	5
RUL of Robot 2 (min)	6.6	5.6	4.6	3.6
Produced (box)	0	10	15	20
RUL of Work Cell 1 (min)	6.6	5.6	4.6	3.6

4.2. Full Implementation of AM-PHM

A more sophisticated implementation of the AM-PHM concept would be to introduce additional features that help convey timely information on the health state of the system. The new features used in this example are the *health balance score*, *average wear state*, *worst wear state*, and *estimated wear state upon completion*. An order to make five boxes was given to the work cell as with the previous example. For the starting health state, only the right drill arm's wear state is at 75 % while all other components are new.

The PHM information from a subordinate component is conveyed to the upper-level AM-PHM module. The collected PHM information is processed to produce the PHM information at the current node. The cutting speed and feed rate parameters are changed to a different operating point within the stable and acceptable range. Work load is changed and the expected results are calculated for all the different parameters. The drill bit wear trend follows the model suggested by Kadirgama et al. (2011). The production rate is changed by adjusting the cutting speed and feed rate which effects the wear rate of the drill bit. According to Furness, Wu and Ulsoy (1996) the feed and speed have relatively small effects on the drill hole quality and that the drilling feed and speed is limited by factors such as drill wear. The drill speed parameters may be adjusted within a certain confine without significantly affecting the hole quality. The final decision is made from the set of choices that best fits the operational directive. The results for this simulation are given in Tables 2 and 3.

For the case in Table 2, the work cell was handed down orders to produce 20 boxes with a directive of minimum health balance. Low balance score means that the components are at a similar state of health and may be used to align maintenance points for the components. The chosen operational profile distributes a load of five boxes for the first robot and 15 boxes for the second robot. However, the cutting speed is adjusted to 100 m/min and the feed rate is also adjusted to 0.1 mm/rot. The production rate is slowed down to 2.1 box/min as a result which reduces the wear of Robot 1’s drill bits to 0.02 mm/min or 6.6 % of its tool life per minute. This results in the production taking approximately 2.1 min.

For the case in Table 3, the work cell is also ordered to produce 20 boxes but with a directive of minimum time. The operational profile chosen suggests a cutting speed of 180 m/min and a feed rate of 0.2 mm/rot. The production rate is increased to 7.6 boxes per minute at the cost of seeing 0.1 mm of flank wear per minute or 33 % of reduction in tool life per minute. The left drill bit reaches its failing point after 30 seconds and the right drilling arm handles the job of drilling holes on the left side as well which reduces the production rate for Robot 1. Production is completed in 1.5 min at an increased cost on the wear of the drill bits.

The AM-PHM methodology is being applied in a simulated environment that is designed to resemble real-world hierarchical manufacturing systems. The canonical example simulation is based on real-world drill bit wear trends. For simplicity, in this paper, tool life is only dependent upon the operating parameters since the material stays consistent. The AM-PHM suggests operating points by optimizing a weighted cost function. The cost function includes all the health related features. The weight used in the cost function is adjusted depending on the decision-maker’s operational directive. The suggested actions such as changes in parameters are based on existing stable operating conditions to ensure system stability.

Table 2. AM-PHM results based on maximum mean health

Time (min)	0	1	2	3
Production Rate of Robot 1 (box/min)	2.1	2.1	2.1	-
RUL of Robot 1 (min)	15.15	14.15	13.15	13
Production Rate of Robot 2 (box/min)	7.6	7.6	7.6	-
RUL of Robot 2 (min)	3	2	1	1
Produced (box)	0	9.7	19.4	20
RUL of Work Cell 1 (min)	15.15	14.15	13.15	13.15

The canonical simulation used in this example is based on models from literature. In the future the AM-PHM methodology will be applied to real-world data some of which is obtained from actual production facilities. The real data will also include a more detailed wear model in which the wear rate is also dependent on additional factors such as current state of wear and material properties.

Table 3. AM-PHM result using maximum health balance and minimum time

Time (min)	0	1	2	3
Production Rate of Robot 1 (box/min)	7.6	5.7	3.8	0
RUL of Robot 1 (min)	3	2	1	1
Production Rate of Robot 2 (box/min)	7.6	7.6	7.6	0
RUL of Robot 2 (min)	3	2	1	1
Produced (box)	0	15.2	20	20
RUL of Work Cell 1 (min)	3	2	1	1

5. Conclusion

The concept of Adaptive Multiscale PHM for manufacturing was introduced in this paper. The AM-PHM methodology calls for the AM-PHM module at each decision point along the hierarchical structure to receive operational profiles outlining the job requirements and report back performance and health estimates appropriate for the upper level.

The AM-PHM is demonstrated on a canonical test manufacturing scenario simulation. Directive oriented decisions were made in the simulation by using additional information on the health of the system in addition to knowledge on the system hierarchical model. The AM-PHM shows promising results as it enables manufacturing work cells to adapt to changing machine conditions.

Further development of the AM-PHM methodology will continue. A modified work cell canonical process is in development. This model is based on a real-world manufacturing facility. A canonical process work cell simulator capable of simulating continuous wear of the components is being developed. The AM-PHM will be tested using this simulation environment and will be compared against other existing PHM based decision-making policies. The results of the different policies will be compared using quantitative measures such as time, monetary cost and Overall Equipment Effectiveness (OEE).

NIST Disclaimer

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

Acknowledgement

This research is supported by the National Institute of Standards and Technology.

References

Ahmad, R., Kamaruddin, S. (2012). An Overview of Time-based and Condition-based Maintenance in Industrial Application. Computers & Industrial Engineering 63, 135-149. doi:10.1016/j.cie.2012.02.002

Al-Habaibeh, A., & Gindy, N. (2000). New Approach for Systematic Design of Condition Monitoring Systems for Milling Processes. Journal of Materials Processing Technology 107 (1-3), 243-251. doi:10.1016/S0924-0136(00)00718-4

Altintas, Y., Verl, A., Brecher, C., Uriarte, L., & Pritschow, G. (2011). Machine Tool Feed Drives. CIRP Annals – Manufacturing Technology 60 (2), 779-796. doi:10.1016/j.cirp.2011.05.010

Barajas, L. G., & Srinivasa, N. (2008). Real-time Diagnostics, Prognostics Health Management for Large-scale Manufacturing Maintenance Systems. ASME International Manufacturing Science and Engineering Conference (85-94), Evanston, IL.

Batzel, T. D., & Swanson, D. C. (2009). Prognostic Health Management of Aircraft Power Generators. IEEE Transactions on Aerospace and Electronic Systems 45, 473-483.

Biehl, S., Staufenbiel, S., Recknagel, S., Denkena, B., & Bertram, O. (2012). Thin Film Sensors for Condition Monitoring in Ball Screw Drives. 1st Joint International Symposium on System-Integrated Intelligence 2012: New Challenges for Product and Production Engineering.

Biswas, G., & Mahadevan, S. (2007). A Hierarchical Model-based approach to Systems Health Management. IEEE Aerospace Conference, March, 3-10. doi: 10.1109/AERO.2007.352943

Borisov, O., Fletcher, S., Longstaff, A., & Myers, A. (2013). New Low Cost Sensing Head and Taut Wire Method for Automated Straightness Measurement of Machine Tool Axes. Optics and Lasers in Engineering 51, 978-985.

Celik, Lee, Vasudevan, and Son (2010) DDDAS-Based Multi-Fidelity Simulation Framework for Supply Chain Systems. IIE Transactions 42, 325-341.

Datta, K., Jize, N., Maclise, D., & Goggin, D. (2004). An IVHM Systems Analysis & Optimization Process. IEEE Aerospace Conference. IEEE (3706-3716).

Feldman, A., de Castro, H. V., and van Gemund A. (2013) Model-Based Diagnostic Decision-Support System for Satellites. IEEE Aerospace Conference. March 2-9, Big Sky, MT.

Ferri, F. A. S., Rodrigues, L. R., Gomes, J. P. P., de Medeiros, I. P., Galvo, R. K. H., & Nascimento, C. L. (2013). Combining PHM Information and System Architecture to Support Aircraft Maintenance Planning. IEEE Systems Conference (60-65), April 15-18, Orlando, FL. doi:10.1109/SysCon.2013.6549859

Furness, R. J., Wu, C. L., & Ulsoy, A. G. (1996). Statistical Analysis of Feed, Speed, and Wear on Hole Quality in Drilling. Journal of Manufacturing Science and Engineering 118, 367-375.

Hofmeister, J. P., Wagoner, R. S., & Goodman, D. L. (2013). Prognostic Health Management (PHM) of Electrical Systems using Conditioned-based Data for Anomaly and Prognostic Reasoning. Chemical Engineering Transactions 33, 991-996.

Holdren, J. P. (2011). Report to the President on Ensuring American Leadership in Advanced Manufacturing. President's Council of Advisors on Science and Technology. https://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-advanced-manufacturing-june2011.pdf

Holland, S. W., Barajas, L. G., Salman, M., & Zhang, Y. (2010). PHM for Automotive Manufacturing & Vehicle Applications. Prognostics & Health Management Conference, Portland, OR.

Hopp, W., & Spearman, M., (3rd). (2008). Factory Physics. Long Grove, IL: Waveland Press, Inc.

Hu, S. J., & Koren, Y. (1997). Stream-of-variation Theory for Automotive Body Assembly. CIRP Annals-Manufacturing Technology 46, 1-6.

International Organization for Standardization, 2002. ISO 13373-1:2002 - Condition Monitoring and Diagnostics of Machines −Vibration Condition Monitoring − Part 1: General Procedures. Genève, Switzerland: International Organization for Standardization.

International Organization for Standardization, 2003. ISO 13374-1:2003 - Condition Monitoring and Diagnostics of Machines − Data Processing, Communication and Presentation − Part 1: General Guidelines. Genève, Switzerland: International Organization for Standardization.

International Organization for Standardization, 2004. ISO 13381-1:2004 - Condition Monitoring and Diagnostics of Machines − Prognostics − Part 1: General Guidelines. Genève, Switzerland: International Organization for Standardization.

International Organization for Standardization, 2012. ISO 13372:2012 - Condition Monitoring and Diagnostics of Machines − Vocabulary. Genève, Switzerland: International Organization for Standardization.

Jalali, S. A., & Kolarik, W. J. (1991). Tool Life and Machinability Models for Drilling Steels. International Journal of Machine Tools and Manufacture 31, 273-282.

Kadirgama, K., Abou-El-Houssein, K. A., Noor, M. M., Sharma, K. V., & Mohammad, B. (2011). Tool life and wear mechanism when machining Hastelloy C-22HS. Wear 270, 258-268.

Liao, L., Minhas, R., Rangarajan, A., Kurtoglu, T., & de Kleer, J. (2014). A Self-Aware Machine Platform in Manufacturing Shop Floor Utilizing MTConnect Data. Annual Conference of the Prognostics and Health Management Society, September 29-October 2, Fort Worth, TX.

Marvel, J. A. (2014). Collaborative Robotics: A Gateway into Factory Automation. ThomasNet News. http://news.thomasnet.com/IMT/2014/09/03/collaborative-robots-a-gateway-into-factory-automation/

Marvel, J. A., Eastman, R., Cheok, G., Saidi, K., Hong, T., & Messina, E. (2012). Technology Readiness Levels for Randomized Bin Picking. Proceedings of the Workshop on Performance Metrics for Intelligent Systems (109-113), March 20-22, College Park, MD. doi:10.1145/2393091.2393114

Marvel, J. A., & Falco, J. A. (2012). Best Practices and Performance Metrics Using Force Control for Robotic Assembly. Gaithersburg, MD: National Institute of Standards and Technology. doi:http://dx.doi.org/10.6028/NIST.IR.7901

Mhenni, F., Nguyen, N., & Choley, J. -Y. (2014). Automatic Fault Tree Generation from SysML System Models. Advanced Intelligent Mechatronics, IEEE/ASME International Conference On (715-720), July 8-11, Besancon, France. doi:10.1109/AIM.2014.6878163

Narasimhan,S., & Brownston, L. (2007). HyDE – A General Framework for Stochastic and Hybrid Model-based Diagnosis. International Workshop on Principles of Diagnosis. May 29-31, Nashville, TN.

National Institute of Standards and Technology. 2015. Measurement Science Roadmap for Prognostics and Health Management for Smart Manufacturing Systems. National Institute of Standards and Technology.

Orcutt, M. (2014). Manufacturers Adding Robots to the Factory Floor in Record Numbers. MIT Technology Review. http://www.technologyreview.com/graphiti/529971/robots-rising/

Peng, Y., Dong, M., & Zuo, M.J. (2010). Current Status of Machine Prognostics in Condition-based Maintenance: a Review. The International Journal of Advanced Manufacturing Technology 50, 297-313.

Philippot, A., Marang, P., Gellot, F., Ptin, J. F., & Riera, B. (2014). Fault Tolerant Control for Manufacturing Discrete Systems by Filter and Diagnoser Interactions. Annual Conference of the Prognostics and Health Management Society, September 29-October 2, Fort Worth, TX.

Sandvik Coromant (2005). *Metalcutting Technical Guide: Turning, Milling, Drilling, Boring, Toolholding; Handbook from Sandvik Coromant.* Sandvik Coromant.

Shen, T., Wan, F., Cui, W., & Song, B. (2010). Application of Prognostic and Health Management Technology on Aircraft Fuel System. Prognostics and System Health Management Conference, IEEE Computer Society. Macau, China.

Snyder, W. E. (1985). *Industrial Robots: Computer Interfacing and Control.* Englewood Cliffs, New Jersey: Prentice-Hall.

SAE International (2009). Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA). J1739_200901, Warrendale, PA: Society of Automotive Engineers International.

Vogl, G. W., Weiss, B. A., & Donmez, M. A. (2014). Standards for Prognostics and Health Management (PHM) Techniques within Manufacturing Operations. Annual Conference of the Prognostics and Health Management Society, September 29-October 2, Fort Worth, TX.

Vogl, G. W., Weiss, B. A., & Donmez, M. A. (2014). Standards Related to Prognostics and Health Management (PHM) for Manufacturing (Tech. Rep.). Gaithersburg, MD: National Institute of Standards and Technology.

Wünsch, D., Lüder, A., & Heinze, M. (2010). Flexibility and Re-configurability in Manufacturing by Means of Distributed Automation Systems – an Overview. In Kühnle, H., Distributed Manufacturing (51-70). London: Springer. doi:10.1007/978-1-84882-707-3

Yoon, J., He, D., & Van Hecke, B. (2014). A PHM Approach to Additive Manufacturing Equipment Health Monitoring, Fault Diagnosis, and Quality Control. Annual Conference of the Prognostics and Health Management Society, September 29-October 2, Fort Worth, TX.

BIOGRAPHIES

Benjamin Y. Choo is in the Ph.D program of the Systems and Information Engineering Department at the University of Virginia (UVa). He received his B.S. and M.S. degree from the Electrical Engineering Department at Yonsei University, Korea in 2005 and 2007 respectively. He received his M.E degree in Electrical Engineering from UVa in 2012. His research interests include manufacturing systems, machine learning and 3D depth sensors.

Dr. Peter A. Beling is an associate professor in the Department of Systems and Information Engineering at the University of Virginia (UVA). Dr. Beling received his Ph.D. in Operations Research from the University of California at Berkeley. Dr. Beling's research interests are in the area of decision-making in complex systems, with emphasis on adaptive decision support systems and on model-based approaches to system-of-systems design and assessment. His research has found application in a variety of domains, including prognostics and health management, mission-focused cybersecurity, and financial decision-making. He is active in the UVA site of the Broadband Wireless Applications Center, which an Industry-University Cooperative Research Center sponsored by the National Science Foundation.

Dr. Amy E. LaViers is an Assistant Professor in Systems and Information Engineering and Director of the Robotics, Automation, and Dance Lab at the University of Virginia. She aims to extract useful features from human movement for robotic applications, such as, endowing co-robots the ability to work alongside human workers in manufacturing plants. Her research began at Princeton University where she earned a certificate in Dance and B.S.E. in Mechanical and Aerospace Engineering. She went on to complete a M.S. and Ph.D. in Electrical and Computer Engineering at the Georgia Institute of Technology.

Dr. Jeremy A. Marvel is a project leader and research scientist in the Intelligent Systems Division of the National Institute of Standards and Technology (NIST) in Gaithersburg, MD. Dr. Marvel received his Ph.D. in 2010 in computer engineering from Case Western Reserve University in Cleveland, OH. Since joining the research staff at NIST, he has established the Collaborative Robotics Laboratory, which is engaged in research dedicated to developing test methods and metrics for the performance and safety assessments of collaborative robotic technologies. His research focuses on intelligent and adaptive solutions for robot applications, with particular attention paid to human-robot collaborations, multi-robot coordination, safety, perception, self-guided learning, and automated parameter optimization. Jeremy is currently engaged in developing measurement science methods and artifacts for the integration and application of robots in collaborative assembly tasks for manufacturing.

Dr. Brian A. Weiss has a B.S. in Mechanical Engineering (2000), Professional Masters in Engineering (2003), and Ph.D. in Mechanical Engineering (2012) from the University of Maryland, College Park, Maryland, USA. He is currently the Associate Program Manager of the Smart Manufacturing Operations Planning and Control program and the Project Leader of the Prognostics and Health Management for Smart Manufacturing Systems project within the Engineering Laboratory (EL) at the National Institute of Standards and Technology (NIST). Prior to his leadership roles in the SMOPAC program and the PHM4SMS project, he spent 15 years conducting performance assessments across numerous military and first response technologies including autonomous unmanned ground vehicles; tactical applications operating on Android devices; advanced soldier sensor technologies; free-form, two-way, speech-to-speech translation devices for tactical use; urban search and rescue robots; and bomb disposal robots. His efforts have earned him numerous awards including a Department of Commerce Gold Medal (2013), Silver Medal (2011), Bronze Medals (2004 & 2008), and the Jacob Rabinow Applied Research Award (2006).

MRS Advances © 2016 Materials Research Society
DOI: 10.1557/adv.2016.122

Impact of Monovalent Counter-ions on the Conformation of Flexible Polyelectrolytes Having Different Molecular Architectures

Alexandros Chremos[1] and Jack F. Douglas[1]
[1]Materials Science and Engineering Division, National Institute of Standards and Technology, Gaithersburg, MD, 20899, U.S.A.

ABSTRACT

We explore the impact of monovalent counter-ions on the molecular conformation of highly charged flexible polyelectrolytes for a range of molecular topologies (linear chains, stars, and unknotted and trefoil rings) by molecular dynamics simulations that include an explicit solvent having short range interaction with the polyelectrolyte. In particular, we investigate how the counter-ions near the polyelectrolytes with variable mass influence the average molecular shape. We also characterize the interfacially "bound" counter-ions by calculating the time-averaged number of interfacial counter-ions, as well as the degree to which the polyelectrolytes wrap around the counter-ions by calculating the number of contacts between the counter-ions and the polyelectrolyte.

INTRODUCTION

Polyelectrolytes are an important class of polymeric molecules that carry charged groups that release counter-ions to an extent that depends on their conformation and charge density when dissolved in polar solvents. Examples include sulfonated polystyrene and polyacrylic acid, as well as, many biological molecules such as DNA and proteins. Insights from the study of these polymers have potential significance in numerous applications, e.g., biomedical implant materials and encapsulating material pharmaceutical drug delivery systems [1, 2]. However, the modeling of synthetic and biological polyelectrolyte solutions is theoretically complicated due to the strong coupling between the counter-ion distribution of and polyelectrolyte conformation [3].

Theoretically, correlations between the counter-ions distribution and the polyelectrolyte are usually described based on the classical counter-ion condensation theory of Manning and subsequent revisions of this classic model of polyelectrolytes [4-7]. According to this theory, when the electrostatic interactions become comparable to thermal energy the counter-ions from their uniform distribution in the solution start to "condense" on the chain backbone, thus largely screening the backbone charge. In the original theory [4, 5], this instability takes place when $\xi = \lambda\, l_B > 1$, (λ is the polyelectrolyte charge per length, and $l_B = e^2 / (\varepsilon_r\, k_B T)$ is the Bjerrum length and ε_r being the solvent dielectric constant). However, Manning theory models polyelectrolytes as infinitely long charged straight threads, while, real polyelectrolytes have a finite chain length and can be relatively flexible. The existence of a flexible backbone raises basic and theoretically unresolved questions about how the polyelectrolyte conformation affects the distribution of counter-ions distributed these polymers and about how the counter-ions, in turn, influence polymer conformation. Simulation studies [8-14] of flexible polyelectrolytes in solution have indicated deviations from the theoretical predictions of Manning theory and emphasize that the counter-ions and polymer conformation are coupled. We can also expect this coupling to be altered by chain topology and solvation (i.e., binding by the solvent to the polymer) that

Chremos, Alexandros; Douglas, Jack.
"Impact of Monovalent Counter-ions on the Conformation of Flexible Polyelectrolytes Having Different Molecular Architectures." Paper presented at the MRS Advances, Boston, MA, Nov 29-Dec 4, 2015.

CAMBRIDGE JOURNALS
http://journals.cambridge.org Downloaded: 26 Feb 2016 IP address: 129.6.154.93

competes with ion association with the polymer. The study of this phenomenon is clearly of practical and fundamental importance.

In the absence of a predictive fundamental theory, we investigate computationally the interdependency between the interfacial counter-ions and the polymer conformational properties of an isolated macro-ion having a range of molecular topologies as a natural starting point for understanding polyelectrolytes. For these model polymers, we quantify the how molecular topology alters the chain conformational properties and determine the average number of counter-ions interfacially associated and contacting the macro-ion. These quantities are generally distinct because individual counter-ions can have multiple contacts with the polyelectrolyte segments. We examine four molecular topologies: linear chains, stars, unknotted rings, and rings with trefoil knots, and we also vary the polymer molecular mass. The simulations are performed with an explicit solvent where the polyelectrolytes are constrained to have a relatively large polymer charge density.

METHODOLOGY

We employ molecular dynamics (MD) simulations based on a bead-spring model of Lennard-Jones (LJ) segments bound by stiff harmonic bonds suspended in explicit LJ solvent, some of which are charged to represent counter-ions and ions from added salt. All macro-ion segments, dissolved ions, and solvent particles are assigned the same mass m, diameter σ, strength of interaction ε, and all dissolved ions are monovalent. We set ε and σ as the units of energy and length and the cutoff distance for LJ interaction potential is $r_c = 2.5\ \sigma$. Polyelectrolyte molecular mass ranges from $M_w = f\ M + 1 = 11$ to 161 segments, where f is the number of arms and M is the number of segments per arm ($f = 2$ for all molecular architecture except for stars). A polyelectrolyte carries a total charge $-Z_p\ e = -\lambda\ M_w\ e$ distributed uniformly along the molecular structure. The polymer segments are connected via a stiff harmonic spring, $V_H(\mathrm{r}) = k(r - l_0)^2$, where $l_0 = \sigma$ is the equilibrium length of the spring, and $k = 1000\ \varepsilon\ /\ \sigma^2$ is the spring constant. To model finite size rods, we use the same model as with flexible chains, but a bending potential is used, $U_{\text{bend}}\ (\theta) = k_{\text{bend}}\ (\theta - \theta_0)^2$; where $\theta_0 = 180^\circ$ and $k_{\text{bend}} = 1000\ \varepsilon\ /\ \mathrm{rad}^2$. All charged particles interact via the Coulomb potential and the particle-particle particle-mesh method is used.

The system is composed of a total of 64 000 solvent particles in a periodic cube of side L. The system includes N_- coions of charge $-e$ and $N_+ = N_- + Z_p$ counter-ions of charge $+e$ so that the system of interest has neutral total charge. Aside from l_B that specifies the strength of the Coulomb interaction, the other key length parameter for an ionic solution is the Debye screening length: $\lambda_D = [4\pi\ l_B\ (\rho_+ + \rho_-)]^{-1/2}$, where $\rho_\pm = N_\pm\ /\ L^3$ are the ion densities. Simulations are conducted for $l_B\ /\ \sigma = 1.85$ and $N_+ = 300$, which results to $\lambda_D\ /\ \sigma \approx 2.5$. The operating conditions are typical of the LJ liquid state: density $\rho\ \sigma^3 = 0.8$ and reduced temperature $k_B\ T\ /\ \varepsilon = 1$, the latter maintained by a Nosé-Hoover thermostat. Typical simulations equilibrate for 2000 τ and data is accumulated over a 7500 τ interval, where $\tau = \sigma\ (m\ /\ \varepsilon)^{1/2}$ is the MD time unit.

CAMBRIDGE JOURNALS
http://journals.cambridge.org Downloaded: 26 Feb 2016 IP address: 129.6.154.93

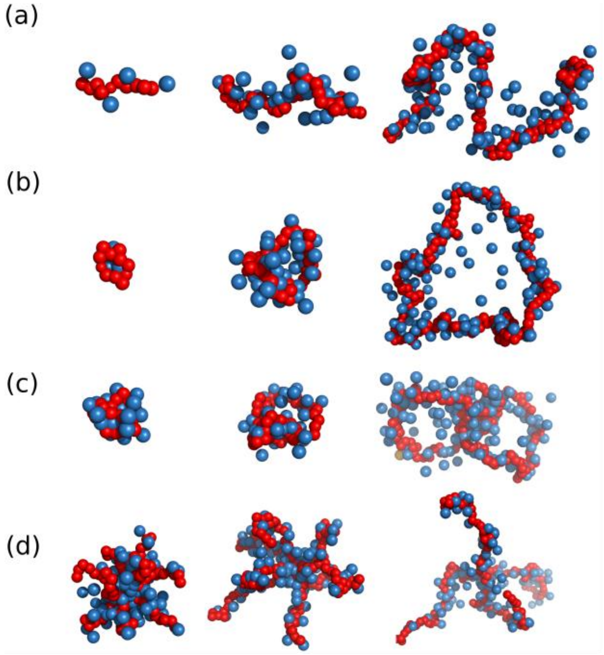


Fig. 1: Screenshots of typical molecular configurations of (a) linear chains; (b) unknotted rings; (c) rings with the trefoil knot; (d) star polymer with f M = 160. The solvent and the majority of the ions are rendered invisible for clarity. For (a-c) and from left to right the molecular mass increases and for (d) the chain functionality decreases with fixed molecular mass.

DISCUSSION

Isolated linear chains with a uniformly distributed charge might be expected to adopt rod-like molecular conformations. Based on this presumed picture, a series of studies have focused on solving Poisson-Boltzmann equation in a cylindrical geometry to estimate the counter-ion distribution [18-20]. However, the chain conformations in real polymer solutions reflect a balance between the repulsion of charged segments of the macro-ion and the covalent bonds between the chain segments so that chain only adopts a rod configuration in an ideal zero-temperature limit where thermal fluctuations can be neglected. To determine to what degree a polyelectrolyte chain resembles a rod-like polymer or a random coil, we compare its shape to a chain with stiff bending potential and a chain without any charges. We use the ratio of the hydrodynamic radius over the radius of gyration, R_h / R_g, which is an often used descriptor to quantify the shape of arbitrary objects; the calculation of R_h is based on the friction coefficient of an arbitrary shaped Brownian particle [21, 22]. The values of R_h / R_g for a smooth sphere is 1.29, for a random walk is 0.79, and for an infinite long rod is 0 [15, 16]. In all cases, the linear chains become more anisotropic as M increases. However, it is clear that polyelectrolyte chains have a relatively stretched “worm-like” configuration with respect to chains having no charges, but nonetheless their shape is quite distinct from a rod (see Fig. 1b for screenshots and Fig. 2), consistent with experimental observations [17]. With respect to the neutral polymers (λ = 0) the ratio decreases for all molecular topologies and range of molecular mass explored. For small M, the polyelectrolytes become more spherical and symmetric since for $M_w \rightarrow 1$ there would be only a single sphere.

CAMBRIDGE JOURNALS
http://journals.cambridge.org Downloaded: 26 Feb 2016 IP address: 129.6.154.93

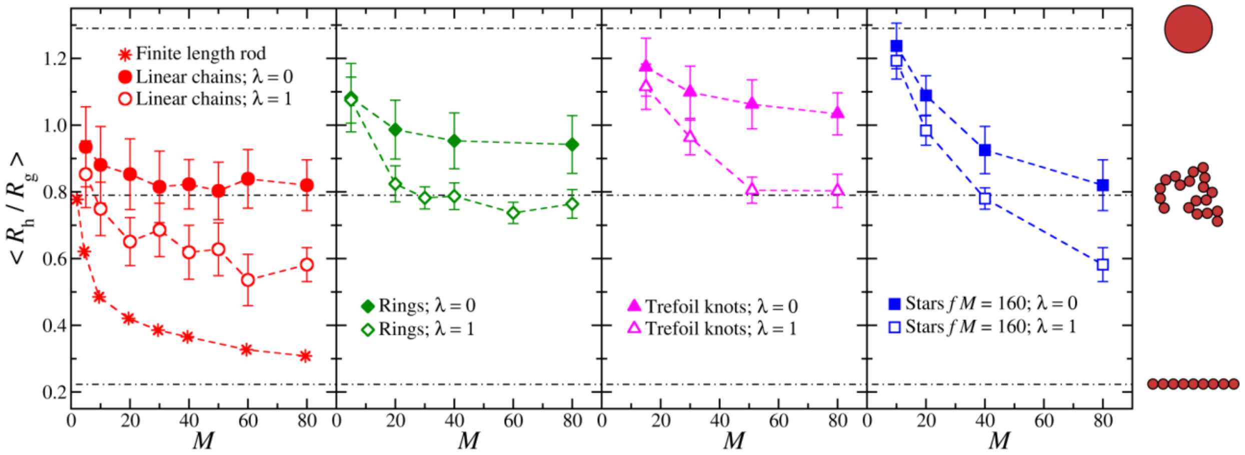


Fig. 2: Ratio of the hydrodynamic radius over the radius of gyration, R_h / R_g, for macromolecules (with charge per segment, λ = 1, and no charge, λ = 0) as function of M. Results for different molecular topologies are also presented. The error bars indicate two standard deviations. The dot-dashed lines correspond to the reference values of primary objects, for a smooth sphere is 1.29, for the rod with an aspect ratio of A = 1550 is 0.22 (see Figure), and for self-avoiding walks in θ-solvent is 0.79 [15, 16].

It is evident from Fig. 1 that the shape (as quantified by R_h / R_g) of our model polyelectrolyte molecules in solution is greatly influenced by molecular topology. For example, the rings resemble “donuts” rather than a rod-like structures. Thermal fluctuations give rise to deviations from this circular loop shape, as seen in Fig. 1b, but overall polyelectrolyte rings retain their donut configuration. Small rings evidently take a more spherical and symmetric shape, Figs. 1 and 2. Note that knotting further enhances this effect (trefoil knot is a unique prime knot with three crossings [23]). As M increases, however, the effect of the topological constraints evidently diminishes. Topological constraints counter-balance the chain stretching caused by the repulsion between the macro-ion charges. The mass dependence of polyelectrolyte trefoil knots reaches a plateau at M ≈ 50 where R_h / $R_g \approx 0.8$, which is curiously close to that of a self-avoiding random walk [16]. We also consider stars, which are molecules having f arms of mass M emanating from the molecular core. By keeping the molecular mass, M_w, of the star polyelectrolytes fixed, $M_w = f\ M + 1 = 161$ and by varying the number of arms, f, we obtain significant changes in R_h / R_g corresponding to a shape from the limit of smooth spheres to flexible chain polyelectrolytes (f = 2), as indicated in Fig. 1e and Fig. 2. Molecular topology evidently greatly alters molecular conformation in highly charged polyelectrolytes; in addition, there are clear differences in terms of shape between charged flexible polyelectrolytes with rod-like structures and with neutral polymers. We next shift our attention to the counter-ions, which largely drive these conformational changes.

The counter-ions “bind” to the polyelectrolyte backbone, which is equivalent to Manning type condensation. The number of interfacial counter-ions with the polyelectrolyte, n_{int}, fluctuates over time reflecting a dynamical binding process. To identify the interfacial counter-ions near the interface, we have used a distance criterion of l_B from any macro-ion segment. Evidently n_{int} is neither independent of molecular mass nor molecular architecture, Fig. 3. This is not surprising given that polyelectrolytes under investigation have a flexible backbone, while in the Manning theory the polyelectrolytes are considered rigid slender needles. Nevertheless, the

CAMBRIDGE JOURNALS
http://journals.cambridge.org Downloaded: 26 Feb 2016 IP address: 129.6.154.93

prediction of Manning theory for the fraction counter-ions that would condense on a charged rod in salt-free case is 1 - 1 / ξ, which is qualitatively consistent with our findings despite obvious differences between the polyelectrolyte systems. The impact of molecular topology is more pronounced for small M, where polyelectrolytes with higher molecular complexity have the tendency to have a higher n_{int} resulting to a more efficient screening of the bare charge. There is evidently a much higher local charge "condensation" on the star and knotted ring polyelectrolytes, which can be attributed to the fact that these structures tend to be more particle-like than chain-like [24]. The molecular topology effect on the charge binding gradually disappears at higher M.

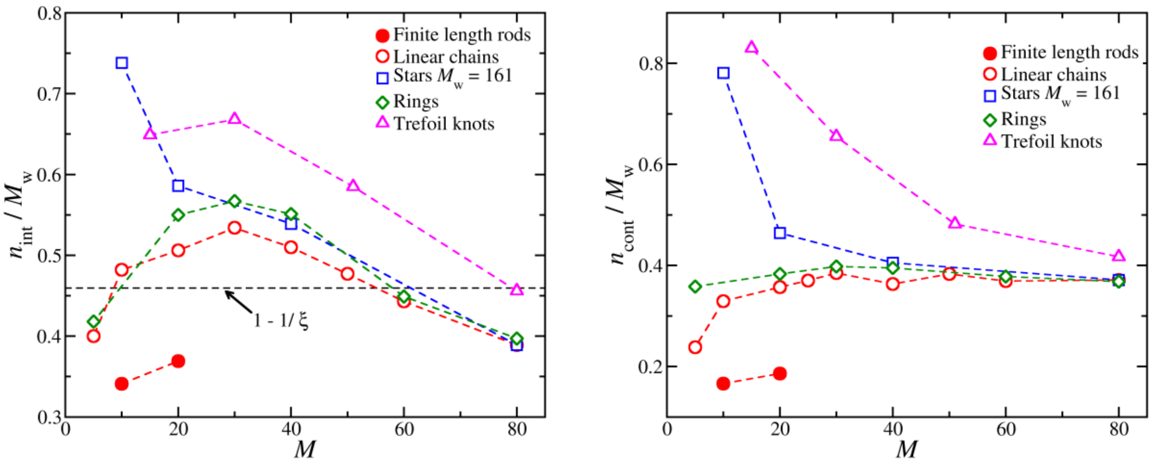


Fig. 3: (Left) Number of interfacial counter-ions, n_{int}, normalized with molecular mass, M_w, as function of the arm molecular mass, M. (Right) Number of contacts the interfacial counter-ions have with the polyelectrolyte, n_{cont}, normalized by M_w, as function of M.

We now focus on the following question: If the fraction of counter-ions do not remain fixed as in Manning theory, then which (if any) quantity remains invariant in this binding process? To probe this question, we narrow down the definition of interfacial counter-ions by considering only counter-ions being whose distance from a macro-ion segment is less or equal to 1.1 σ. We calculated the average number of contacts the interfacial counter-ions have with the polyelectrolyte chain, n_{cont}. While we find similar features as in the case of n_{int}, n_{cont} approaches to the same saturation level $n_{\text{cont}} / M_w \approx 0.37$ for all molecular topologies, which reflects the degree of chain "coiling" around counter-ions. In other words, this suggests that higher molecular mass polyelectrolyte chains become more flexible and adopt molecular conformations that coil around the counter-ions. Moreover, for chains we observe conformational transition at about $M \approx 30$. A similar conformational transition between rod-like conformations and flexible coil was recently discussed for the charged bipolymer DNA [25] and even unentangled linear alkane chains [26]. Ring polyelectrolytes exhibit similar trends for n_{int} and n_{cont}, but stars and trefoil knots attract more counter-ions and at the same time coil more efficiently.

CONCLUSIONS

In summary, we investigated the impact of monovalent counter-ions around polyelectrolytes having a range of topologies. While we find a well-defined fraction of counter-ions near the surface of the polyelectrolyte as anticipated by the Manning condensation theory,

Chremos, Alexandros; Douglas, Jack.
"Impact of Monovalent Counter-ions on the Conformation of Flexible Polyelectrolytes Having Different Molecular Architectures." Paper presented at the MRS Advances, Boston, MA, Nov 29-Dec 4, 2015.

CAMBRIDGE JOURNALS
http://journals.cambridge.org Downloaded: 26 Feb 2016 IP address: 129.6.154.93

this fraction is significantly influenced by molecular topology, a phenomenon that Manning theory cannot address. In particular, an increase in the molecular complexity leads to an increase of the number of interfacial counter-ions resulting to a more efficient screening of the bare charge. We expect that this effect should have a large influence on the propensity of the polyelectrolytes to undergo supramolecular assembly into large scale domains, a ubiquitous, but theoretically unexplained property of many synthetic and biological polyelectrolytes [27]. We also find that the chain contacts the interfacial counter-ions remains remarkably invariant, suggesting that the backbone chain "coils" around these counter-ions. This phenomenon should be even more prevalent for higher valent counter-ions and can be expected to influence the rigidity of the polyelectrolyte. We plan to investigate this effect in future work.

AKNOWLEDGEMENTS

Financial support was provided by the NIST Fellow Postdoctoral Program. Official contribution of the U.S. National Institute of Standards and Technology -- not subject to copyright in the United States.

REFERENCES

1. A. Yethiraj, J. Phys. Chem. B **113**, 1539 (2009).
2. A. V. Dobrynin and M. Rubinstein, *Prog. Polym. Sci.* **30**, 1049 (2005).
3. V. M. Prabhu, *Curr Opin. Colloid Interface Sci.* **10**, 2 (2005).
4. G. S. Manning, *J. Chem. Phys.* **51**, 924 (1969).
5. G. S. Manning, *J. Chem. Phys.* **51**, 3249 (1969).
6. D. Stigter, *Biophysical J.* **69**, 380 (1995).
7. A. Deshkovski, S. Obukhov, and M. Rubinstein, *Phys. Rev. Lett.* **86**, 2341 (2001).
8. M. J. Stevens and K. Kremer, *J. Chem. Phys.* **103**, 1669 (1995).
9. J. C. Chu and C. H. Mak, *J. Chem. Phys.* **110**, 2669 (1999).
10. H. J. Limbach and C. Holm, *J. Chem. Phys.* **114**, 9674 (2001).
11. S. Liu and M. Muthukumar, *J. Chem. Phys.* **116**, 9975 (2002).
12. M. Ullner and C. E. Woodward, *Macromolecules* **35**, 1437 (2002).
13. T. S. Lo, B. Khusid, and J. Koplik, *Phys. Rev. Lett.* **100**, 128301 (2008).
14. J.-M. Y. Carrillo and A. V. Dobrynin, *Macromolecules* **44**, 5798 (2011).
15. M. L. Mansfield and J. F. Douglas, *Macromolecules* **41**, 5422 (2008).
16. M. L. Mansfield and J. F. Douglas, *J. Chem. Phys.* **139**, 044901 (2013).
17. B. Schuler, *et al.*, *Proc. Natl. Acad. Sci. U.S.A.* **102**, 2754 (2005).
18. M. Deserno, C. Holm, and S. May, *Macromolecules* **33**, 199 (2000).
19. M. Deserno and C. Holm, *Mol. Phys.* **100**, 2941 (2002).
20. R. D. Groot, *J. Chem. Phys.* **95**, 9191 (1991).
21. J. B. Hubbard and J. F. Douglas, *Phys. Rev. E* **47**, 2983 (1993).
22. M. L. Mansfield, J. F. Douglas, and E. J. Garboczi, *Phys. Rev. E* **64**, 061401 (2001).
23. L. H. Kauffman, Knots and Physics (World Scientific, 1991).
24. A. Chremos and J. F. Douglas, *J. Chem. Phys.* **143**, 111104 (2015).
25. M. L. Mansfield, A. Tsortos, and J. F. Douglas, *J. Chem. Phys.* **143**, 124903 (2015).
26. C. Jeong and J. F. Douglas, *J. Chem. Phys.* **143**, 144905 (2015).
27. Y. Zhang, J. F. Douglas, B. D. Ermi, and E. J. Amis, *J. Chem. Phys.* **114**, 3299 (2000).

Chremos, Alexandros; Douglas, Jack.
"Impact of Monovalent Counter-ions on the Conformation of Flexible Polyelectrolytes Having Different Molecular Architectures." Paper presented at the MRS Advances, Boston, MA, Nov 29-Dec 4, 2015.

http://journals.cambridge.org Downloaded: 26 Feb 2016 IP address: 129.6.154.93

Optofluidic Temperature and Pressure Measurements with Fiber Bragg Gratings Embedded in Microfluidic Devices

G. A. Cooksey and Z. Ahmed
National Institute of Standards and Technology (NIST), Sensor Science Division
100 Bureau Drive, Gaithersburg, MD 20899
zeeshan.ahmed@nist.gov

ABSTRACT

The integration of photonic sensors into microfluidic devices provides opportunities for dynamic measurement of chemical and physical properties of fluids in very small volumes. We previously reported on the use of commercially available Fiber Bragg Gratings (FBGs) and on-chip silicon waveguides for temperature sensing. In this report, we demonstrate the integration of FBGs into easy-to-fabricate microfluidic devices and report on their sensitivity for temperature and pressure measurement in microliter volumes. These sensors present new routes to measurement in microfluidic applications such as small-volume calorimetry and microflow metrology.

Keywords: optofluidics, microfluidics, temperature, pressure, photonic sensors

1 INTRODUCTION

Microfluidic platforms provide sub-microliter control of fluid transport and mixing of chemicals over a broad range of length and time scales. However, characterization of fluids processed in microfluidic devices is generally performed with macroscale systems. Much effort is now focused on integrating measurement systems that can rapidly interrogate the composition and physical properties of fluids within the microfluidic systems themselves, where rapid sensing and dynamic decisions can be made while fluids are still on the chip.

Photonic sensing technologies are particularly promising for microfluidics because they facilitate a broad array of sensing modalities and are compatible with the scale of microfluidic systems. Fiber Bragg Gratings (FBGs) are commercially available photonic sensing devices that have high sensitivity to changes in temperature and mechanical strain [1]. In addition, research and development of smaller chip-scale technologies, such as ring resonators or photonic crystal cavities, are taking measurements into even smaller spaces and providing opportunities for parallelization and high-throughput multifunctional sensing platforms [2, 3].

Microscale photonic devices are well matched in scale to couple with microfluidics, but as with microelectromechanical systems, there can be challenges integrating different platforms and material types. We have focused on rapid prototyping with tapes and laminates as a simple method to build and test devices without need of sophisticated equipment [4]. Overall, we demonstrate these devices sense small changes in temperature and pressure that present new opportunities for thermodynamic and mechanical interrogation of microfluidic processes.

2 EXPERIMENTAL

The optofluidic devices used in this study are easy to fabricate and assemble with off-the-shelf components. Poly(dimethylsiloxane) (PDMS) membranes were purchased (Interstate Specialty Products)† or cured from spun-coat PDMS (Sylgard 184, 10:1 base:crosslinker, Dow Corning). Double-sided silicone tape (#96042, 3M™) was used to adhere layers together and was also cut with a plotter razor cutter (FC800, Graphtech) or laser machine (VLS2.30 VersaLASER, Universal Laser Systems) to form microfluidic channels and channels for FBG insertion [4]. Glass slides and acrylic films (McMaster-Carr) were used as substrates and covers, respectively.

Commercially available FBGs with Bragg resonance in the range of 1540 nm to 1560 nm (os1100, Micron Optics) were adhered in microchannels or cured into spin-cast PDMS membranes of approximately the same thickness as the fiber diameter. We have described in detail elsewhere the experimental system to interrogate photonic devices [5, 6]. Briefly, peak resonance of FBGs was determined after scanning a laser over the resonance region and measuring the power of the reflected signal. Fluid temperatures were controlled using a temperature-controlled water bath. Fluid pressure was controlled using the height of water in a reservoir with additional pressure provided by a pressure controller (PSD-15PSIG, Alicat Scientific) over the reservoir.

3 RESULTS AND DISCUSSION

A temperature sensing microfluidic device was fabricated by embedding a FBG under a 500 µm wide microfluidic channel (**Figure 1**). The microchannel spanned approximately 8 mm of the 10 mm grating region and contained ≈ 2 µL of fluid above the FBG sensor. We calibrated the temperature and sensitivity of the fiber in

Cooksey, Gregory; Ahmed, Zeeshan.
"Optofluidic Temperature and Pressure Measurements with Fiber Bragg Gratings Embedded in Microfluidic Devices."
Paper presented at the TechConnect World Innovation Conference & Expo, Washington, DC, May 22-May 25, 2016.

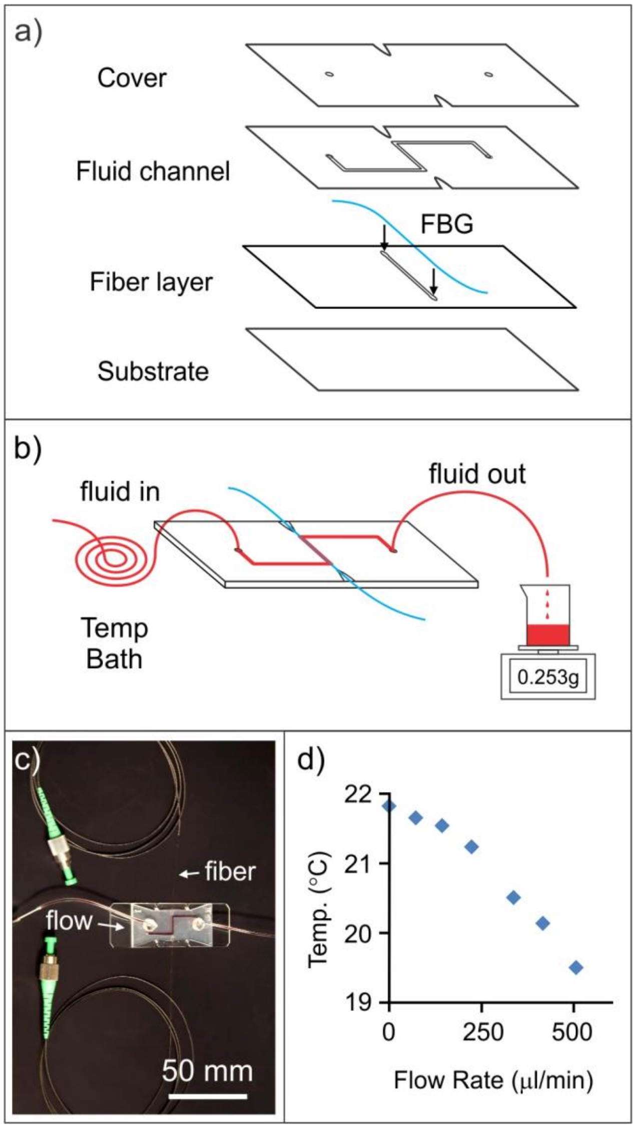


Figure 1. ***(a)*** *Exploded view of optofluidic device shows the various layers constructed from laser-cut tapes and laminates.* ***(b)*** *The optofluidic chip layout delivers temperature-controlled liquids over a FBG through a microfluidic channel. Flow was measured by collecting fluid on a microbalance.* ***(c)*** *Photograph of the completed device with FBG and red dye loaded in the microchannel. (**d**) Heat transfer into the device was controlled by modifying the flow of ice water into the chip. The estimated mean temperature at the FBG is plotted against the flow delivering cold liquid into the 22 ℃ device.*

the chip by measuring the Bragg resonance after submersing the entire chip in controlled temperature baths from 4 °C to 25 °C. In this temperature range, we determined a resonance shift of 17.9 pm/°C. This value is nearly double the manufacturer specification of 10 pm/°C, which we believe indicates that the FBG is strained due to thermal expansion of the chip. Sensitivity of the FBG to changing temperatures of fluid in the microchannel was tested by flowing ice water into the chip at different flow rates, while the chip was held at 22 °C. Faster flows resulted in more heat transfer to the sensing region of the microchannel. Peak resonances were mapped to the calibrations in order to estimate the mean temperature at the sensor (**Figure 1d**). It is important to point out that the FBG is not fully exposed to the flowing liquid – it is only exposed at the bottom of the fluid channel and is otherwise buffered by the chip. Thus, the fiber measures only a fraction of the difference between the liquid and chip temperatures. Flows of 500 µL/min dropped the mean temperature of the FBG to about 19 °C. We did not test faster flows, but the data indicate that the sensor has not been maximally cooled by the flowing water.

Previously, we determined the temperature uncertainty of FBGs in our measurement system was on the order of 0.5 °C [6]. The optofluidic chip demonstrates the capacity to sense perhaps even smaller relative temperature changes, but more work is needed to understand temperature distributions along the microchannel and around the FBG, which was only partially exposed to the cold liquid. It is important to note, however, that compared to macroscale thermometry measurements, the system volume has been reduced to 2 µl above the sensor, which is a reduction of nearly 5 orders of magnitude. Our work indicates an in-channel optical sensor could be used to perform sensitive thermo-chemical measurement, *e.g.* monitoring enthalpic changes due to pseudo-polymorphic transitions in crystalline materials [7].

We initially buried the FBG in a microchannel below the fluid channel as a way to precisely control its position; however, placing the fiber directly in the channel should improve temperature sensitivity by increasing the surface contact with the fiber while reducing the volume flow through the channel. Even smaller channels, nearer to the size of the fiber, could be achieved using higher resolution fabrication strategies, such as soft lithography [8]. Although we controlled heat transfer to the sensor by changing the fluid flow, the device could also be operated as a flow meter by measuring heat transfer and calibrating to determine flow.

Because FBGs are also quite sensitive to mechanical strain, we tested the feasibility of using FBGs as pressure sensors within microfluidic devices. We designed a microfluidic device that incorporated a FBG into a flexible membrane made of PDMS and positioned it below a microchannel. The microchannel above the FBG was expanded to a 2 mm diameter region that could deflect downward into an open region below the membrane (**Figure 2**). Increasing fluid pressure deflected the membrane into open space below the chamber, which strained the fiber and shifted the Bragg wavelength. We tested input fluid pressures ranging from 0 kPa to 75 kPa (0 psi to 10.9 psi), which cover typical pressures for microfluidic applications [9]. The device was sensitive to

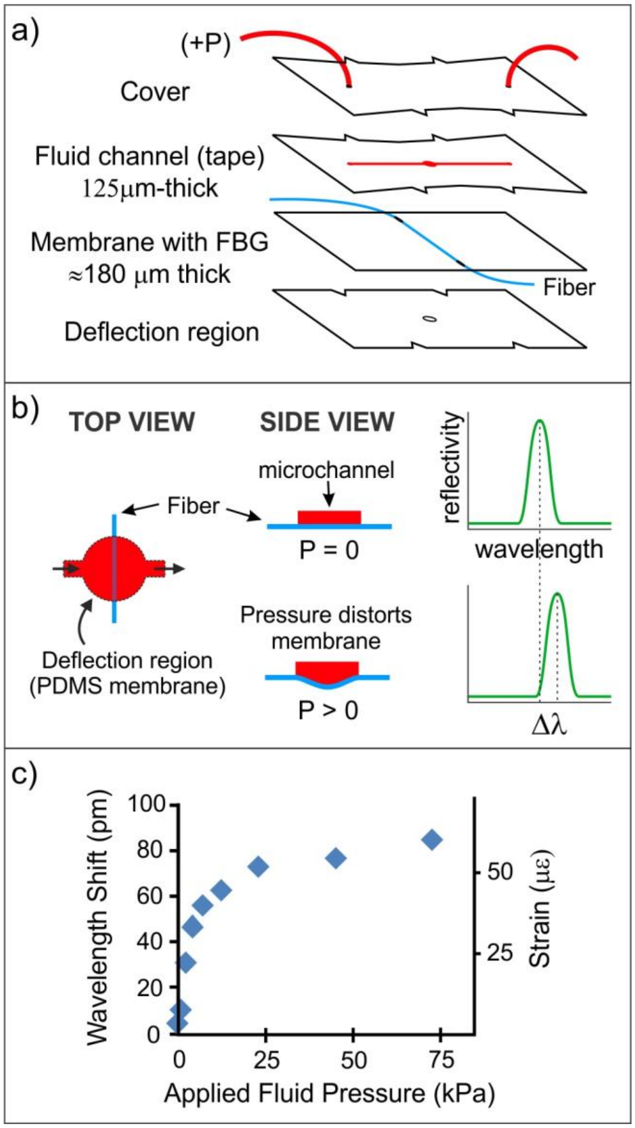


***Figure 2. (a)** Exploded view of layers involved in making the pressure sensing microfluidic device. P is applied pressure. **(b)** An FBG (blue) embedded in a flexible membrane responds to strain applied via a microfluidic channel (red) and deflects down into an open chamber. Bragg resonance shift is depicted in green traces. **(c)** Bragg resonance peak shift (and equivalent stress) is shown as a function of pressure applied to the input fluid. Wavelength shift is converted to strain based on manufacturer specification of 1.4 pm/με.*

pressure changes in the microchannel on the order of about 700 Pa (0.1 psi) although the wavelength shift decreased as pressures eclipsed 5 kPa.

Further characterization of the pressure sensor is needed. We would like to better understand how membrane deformation relates to the strain on the FBG. It is unclear if the saturation of the Bragg wavelength shift above 25 kPa applied pressure is related to the membrane reaching peak deformation into the deflection region. Because we see the membrane deflecting around the fiber, we are in the process of determining if a more rigid membrane material would expand the dynamic range of the system. We are also looking at the reproducibility of these measurements given that fiber alignment over the deflection region will likely influence sensor performance.

4 SUMMARY

This work demonstrates easy-to-build optofluidic systems that enable measurements of small temperature and pressure changes in microliter volumes. These sensing systems provide on-chip assessment of flow and heat transfer, which enables improvement in fluid metrology and permits new opportunities in microscale calorimetry and advanced biological sensing.

†DISCLAIMER

Certain commercial products are identified in this report to adequately specify the experimental procedure. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

REFERENCES

[1] Othonos A. (1997). “Fiber Bragg gratings” *Rev Sci Instr*. **68**, 4309.

[2] Baker JE, Sriram R, Miller BL. (2015). “Two-dimensional photonic crystals for sensitive chemical and biochemical sensing.” *Lab Chip* **15**, 971-990.

[3] Bogaerts W, De Heyn P, Van Vaerenbergh T, et al. (2012). “Silicon Microring Resonators.” *Laser Photonics Rev*. **6**(1), 47-73.

[4] Cooksey GA, Atencia J. (2014). “Pneumatic valves in folded 2D and 3D fluidic devices made from plastic films and tapes.” *Lab Chip* **14**(10), 1665 - 1668.

[5] Xu H, Hafezi M, Fan J, Taylor JM, Strouse GF, Ahmed Z. (2014). “Ultra-sensitive chip-based photonic temperature sensor using ring resonator structures.” *Optics Express* **22**(3), 3098-3104.

[6] Ahmed Z, Filla J, Guthrie W, Quintvalle J. (2015). “Fiber Bragg Grating Based Thermometry.” *NCSLI Measure J. Meas. Sci*. 10(4), 21-27.

[7] Ahmed Z, Chou SG, Siegrist K, and Plusquellic DF. (2011). "State-resolved THz spectroscopy and dynamics of crystalline peptide-water systems." *Faraday Discussions* **150**, 175-192.

[8] Duffy DC, McDonald JC, Schueller OJA, Whitesides GM. (1998). *Anal. Chem*. **70**, 4974-4984.

[9] Au AK, Lai H, Utela BR, Folch A. (2011). “Microvalves and micropumps for BioMEMS.” *Micromachines* **2**, 179-220.

Probing Charge Transfer and Hot Carrier Dynamics in Organic Solar Cells with Terahertz Spectroscopy

Paul D. Cunningham*,[a], Paul A. Lane[a], Joseph S. Melinger[a], Okan Esenturk[b], Edwin J. Heilweil[c]
[a]U.S. Naval Research Laboratory, Washington, DC 20375, United States;
[b]Chemistry Department, Middle East Technical University, Ankara, Turkey;
[c]National Institute of Standards and Technology, Gaithersburg, MD 20899, United States.
*paul.cunningham@nrl.navy.mil

ABSTRACT

Time-resolved terahertz spectroscopy (TRTS) was used to explore charge generation, transfer, and the role of hot carriers in organic solar cell materials. Two model molecular photovoltaic systems were investigated: with zinc phthalocyanine (ZnPc) or alpha-sexathiophene (α-6T) as the electron donors and buckminsterfullerene (C_{60}) as the electron acceptor. TRTS provides charge carrier conductivity dynamics comprised of changes in both population and mobility. By using time-resolved optical spectroscopy in conjunction with TRTS, these two contributions can be disentangled. The sub-picosecond photo-induced conductivity decay dynamics of C_{60} were revealed to be caused by auto-ionization: the intrinsic process by which charge is generated in molecular solids. In donor-acceptor blends, the long-lived photo-induced conductivity is used for weight fraction optimization of the constituents. In nanoscale multi-layer films, the photo-induced conductivity identifies optimal layer thicknesses. In films of ZnPc/C_{60}, electron transfer from ZnPc yields hot charges that localize and become less mobile as they thermalize. Excitation of high-lying Franck Condon states in C_{60} followed by hole-transfer to ZnPc similarly produces hot charge carriers that self-localize; charge transfer clearly precedes carrier cooling. This picture is contrasted to charge transfer in α-6T/C_{60}, where hole transfer takes place from a thermalized state and produces equilibrium carriers that do not show characteristic signs of cooling and self-localization. These results illustrate the value of terahertz spectroscopic methods for probing charge transfer reactions.

Keywords: terahertz spectroscopy, carrier dynamics, organic solar cells

1. INTRODUCTION

The performance of organic solar cells has significantly improved in recent years, with power conversion efficiencies exceeding 10%.[1, 2] In order to achieve these and further gains, much attention has been given to understanding the influence of the sample morphology[3-5] and of charge transfer states[6] on photocurrent generation and loss mechanisms. It is clear that both play important roles in the rapid charge generation that would otherwise seem at odds with the excitonic nature of organic semiconductors. However, a debate has emerged as to whether efficient charge separation occurs via hot charge transfer excitons or energy-gradient driven molecular hopping. While many ultrafast spectroscopic measurements show increasing evidence for the important role of hot charge transfer excitons,[7] device-like charge collections measurements show no significant gains from hot excitations.[8] Central to this debate is the question of whether large donor-acceptor energy level offsets are needed to generate efficient photocurrent. The answer to this question has consequences for efforts aimed at increasing the open circuit voltage of organic photovoltaic cells.[9]

The excitonic nature of organic semiconductors stems from their low dielectric constants and strong electron-phonon interactions. The former leads to unscreened Coulombic attraction between electrons and holes, and the latter leads to structural relaxation of the excited state into a lower energy configuration. In order to separate charges, energetically downhill charge transfer reactions are engineered into organic solar cells. Typically charge transfer occurs at a donor-acceptor heterojunction where the energy-level offset overcomes the exciton binding energy and favorable reorganization energies inhibit back transfer. The state that initially forms upon charge transfer is a charge transfer exciton (CTE), comprised of a hole in the donor and an electron in the acceptor that are held by mutual attraction at the donor-acceptor interface. Within Onsager theory, the interaction between electrons and holes is governed by a Coulombic potential that is inversely proportional to dielectric constant and electron-hole separation. Delocalization

Cunningham, Paul; Lane, Paul; Melinger, Joseph; Esenturk, Okan; Heilweil, Edwin.
"Probing Charge Transfer and Hot Carrier Dynamics in Organic Solar Cells with Terahertz Spectroscopy."
Paper presented at SPIE Commercial + Scientific Sensing and Imaging, Baltimore, MD, Apr 17-Apr 21, 2016.

increases the electron-hole separation and weakens the mutual attraction, increasing the probability that the CTE dissociates into separate charges. So-called “hot” CTE states with excess energy are more delocalized, which is thought to be a key factor in driving charge separation.[7, 10] Entropy considerations may also play a role, through the increase in multiplicity of charge-separated states available to delocalized CTEs.[11] Due to the required reorganization energy, Marcus theory suggests that an optimum excess energy may exist, above which CTEs dissociate with lower probabilities.[12] Hot CTEs may be important only if the rate of charge separation is higher than the rate of thermalization. If instead, the CTE cools prior to energy transfer, other factors may influence efficient charge separation from relaxed CTEs.[8] Local morphology may play an important role in increasing delocalization, independent of CTE energy.[13] High charge carrier mobility may also help CTE dissociation by similarly contributing to increased delocalization and inhibiting geminate recombination. Finally, internal electric fields may reduce the barrier to charge separation in the downfield direction, thus increasing the charge separation probability. It is not yet clear to what degree each of these factors contributes to charge separation.

Here we examine charge transfer in two model molecular donor-acceptor systems comprised of either zinc phthalocyanine (ZnPc) or α-sexithiophene (α-6T) as an electron donor and Buckminsterfullerene (C_{60}) as the electron acceptor. High efficiency organic photovoltaic cells have been achieved using thiophenes and phthalocyanines.[14] The energy level offsets in each donor-acceptor system allow for the important role of excess driving energy to be explored. We apply both transient absorption and time-resolved terahertz spectroscopy to monitor the photogenerated excited state species as well as the photo-induced conductivity. Together, this provides insight into the evolution of the populations of excitons and charge separated species as well as the transient charge carrier mobility. By varying the excitation photon energy, we can compare the results of creating either hot or cool charge transfer excitons in order to determine the role of excess energy on charge separation.

2. METHODOLOGY

ZnPc, α-6T, and C_{60} were purified by vacuum train sublimation prior to use. Organic thin films (~300nm thick) were deposited onto quartz substrates by thermal evaporation under vacuum (10^{-7} Torr). Composite films were prepared by co-sublimation while those consisting of nanometer-thick layers were prepared by alternating layer deposition of the constituents. Layer thicknesses varying from 1 nm to 10 nm were determined using a quartz crystal microbalance. The optical absorption spectrum was measured with a spectrophotometer, while measurements at optical density < 0.1 were conducted using a custom spectrometer with an integrating sphere.

Transient absorption (TA) measurements were based on a 1kHz Ti:Sapphire amplifier with a fundamental wavelength of 775 nm whose output was split to generate excitation and probe pulses. The frequency-doubled output was used for photo-excitation, while the excited state spectra were measured using a while light continuum probe generated in a sapphire plate. The white-light probe was sent through a scanning monochromator, which allows for the excited state spectrum to be recorded as well as for specific probe wavelengths, e.g. corresponding to the ground state bleach (GSB) or excited state absorption (ESA), to be selected. The dynamics of these excited-state populations were recorded by varying the delay, i.e. optical path length, between the excitation and probe pulses using a mechanical delay stage.

Time-resolved terahertz spectroscopy (TRTS)[15] was based on a 1kHz Ti:Sapphire amplifier with a fundamental wavelength of 800 nm and a 60 fs pulse width whose output was split to generate excitation and probe pulses. Optical excitation pulses were generated either by frequency-doubling the output to 400 nm or by pumping a near-infrared optical parametric amplifier that was subsequently frequency-doubled to 615 nm. Terahertz (THz) probe pulses were generated by optical rectification in a 2 mm thick [110] ZnTe crystal and coherently detected by free-space electro-optic sampling in a second ZnTe crystal. Coherent detection of the THz probe pulse electric field allows for simultaneous determination of the refractive index and absorption, or equivalently the complex conductivity.

Photo-induced conductivity dynamics were recorded by monitoring the change in the peak THz waveform electric field amplitude as a function of time after photo-excitation. This is done by first fixing the delay, i.e. optical path length, between the pulse that generates the THz waveform and the pulse that samples its electric field amplitude, then scanning the delay between the excitation pulse and the THz pulse. It can be shown that the change in the peak THz electric field is proportional to the changes in the real conductivity, while photo-induced phase shifts more easily measured at the zero-crossing of the THz electric field are dominated by changes in the imaginary conductivity.[16] The complex frequency-dependent conductivity was extracted from scans measuring the change in the transmitted THz pulse at a given delay after photo-excitation using the thin film approximation.[17] All measurements were performed in a dry-air purged box to minimize THz absorption by atmospheric water vapor.

3. RESULTS

First we examine the excited state behavior of neat C_{60} films, Figure 1a. Photo-excitation at 400 nm (3.1 eV) leads to an instrument limited rise in photo-induced conductivity measured via TRTS. This is followed by an ultrafast exponential decay (500 fs) to a slowly decaying residual conductivity. These dynamics were absent from both C_{60} in solution and C_{60} isolated in a polystyrene matrix,[18] implying that they do not originate from intramolecular excited states. On the other hand, photo-excitation of C_{60} at 615 nm (2 eV) yields no observable photo-induced conductivity. This indicates that there is a threshold energy necessary to produce charge separated species in C_{60}. Early studies of C_{60} reported a 2.3 eV threshold for transient photocurrent,[19] suggesting the existence of intermolecular charge transfer states. Excited state dynamics in C_{60} probed at 550 nm (2.25 eV) via TA, which was previously assigned to charge transfer excitons (CTE),[20] show a multiexponential decay with an initial fast component that matches the photo-induced conductivity decay. Therefore, we conclude that this photo-induced conductivity decay is dominated by recombination and not changes in mobility.

We assign the C_{60} dynamics to autoionization,[21] which is the intrinsic method of charge carrier generation in organic solids. Here, excitation to a higher-lying Franck-Condon state allows for charge transfer to a neighboring molecule of the same type. The created geminate pair can then either recombine or escape the Coulomb potential via a thermally-activated process to form charge carriers, Figure 1b. In terms of Onsager theory, the excess energy of this hot CTE increases the electron-hole separation and thus the probability of charge separation. The fast photo-induced conductivity and CTE population decays are consistent with hot CTE relaxation times.[11, 22, 23] Here, many electrons do not escape the Coulomb potential and the hot CTE undergoes a form of self-trapping as it cools. The resulting bound CTE has insufficient polarizability to significantly absorb at THz frequencies.[17, 24] From our measurements, we infer that the 0.3 eV excess energy above the absorption edge that is given to an exciton upon 615 nm exciton is insufficient for autoionization.

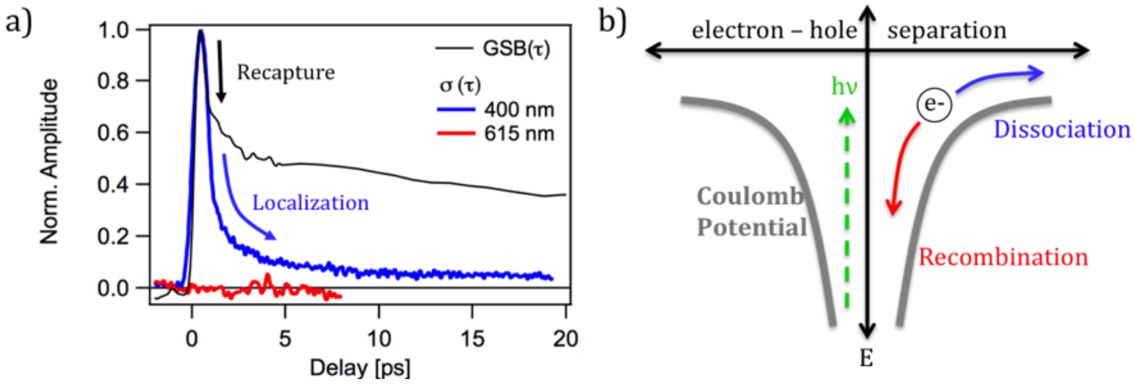


Figure 1. (a) Ground state bleach probed at 550 nm (black) and TRTS conductivity dynamics in C_{60} resulting from 400 nm (blue) and 615 nm (red) excitation. (b) Schematic of the autoionization process where higher excitation energies lead to greater delocalization and a higher probability of exciton dissociation.

Next we examine the ZnPc:C_{60} donor:acceptor system. In both the blends and nanoscale multilayered films, bi-exponential photo-induced conductivity dynamics are observed. No photoinduced conductivity response is observed in neat ZnPc, which recent measurements suggest may require a higher degree of crystallinity than achieved through sublimation in order to provide significant delocalization and support long-range charge separation.[25] The rapid initial decay of the photo-induced conductivity is absent from the excited state dynamics of the multilayered films probed at 550 nm, which corresponds to transitions of the ZnPc cations, Figure 2a. The observed linear fluence dependence indicates that the fluences used here are not sufficiently high as to produce polaron pair annihilation, which can lead to rapid recombination.[26] The lack of correlation between the excited state and conductivity dynamics indicates that the later is dominated by changes in mobility following charge transfer.[27] Here, the transferred charge carriers possess excess energy and greater mobility, which decreases as the carriers cool and become more localized. This is consistent with recent measurements showing that carriers are generated within 100 fs in polymer:fullerene blends and localize within 1 ps as they thermalize.[28] The excited state and photoinduced conductivity dynamics are correlated for delays > 20 ps, where recombination dominates the changes in conductivity.[21]

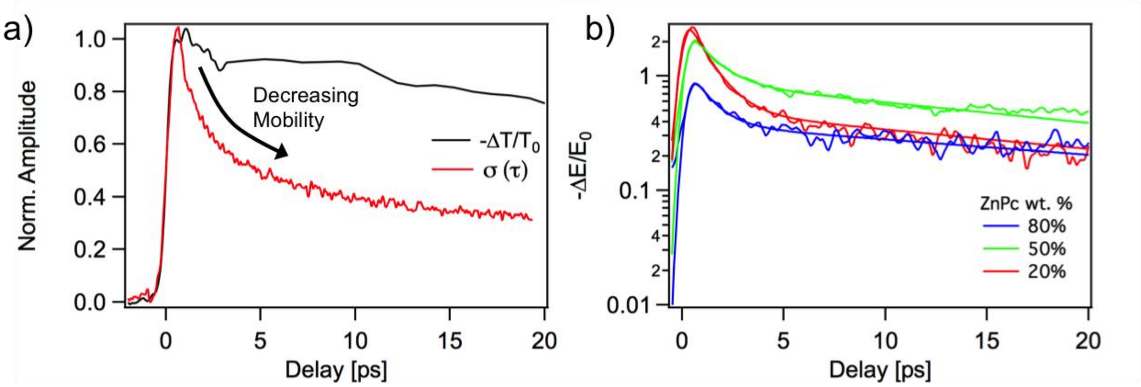


Figure 2. (a) ZnPc cation dynamics (black) measured via TA at 550 nm and conductivity dynamics (red) measured via TRTS in the ZnPc:C_{60} donor:acceptor system. (b) TRTS conductivity dynamics in ZnPc:C_{60} co-sublimed films as a function of the percent weight of ZnPc.

The long-lived component of the photoinduced conductivity, which is proportional to the charge carrier concentration, exhibits a clear dependence on the blend composition for ZnPc:C_{60}, Figure 2b. The optimum weight fraction is found to be 50% donor and 50% acceptor.[18] This may be related to the need for both a sufficiently crystallized donor[29] and large acceptor domain sizes[13] in order to achieve efficient charge separation.

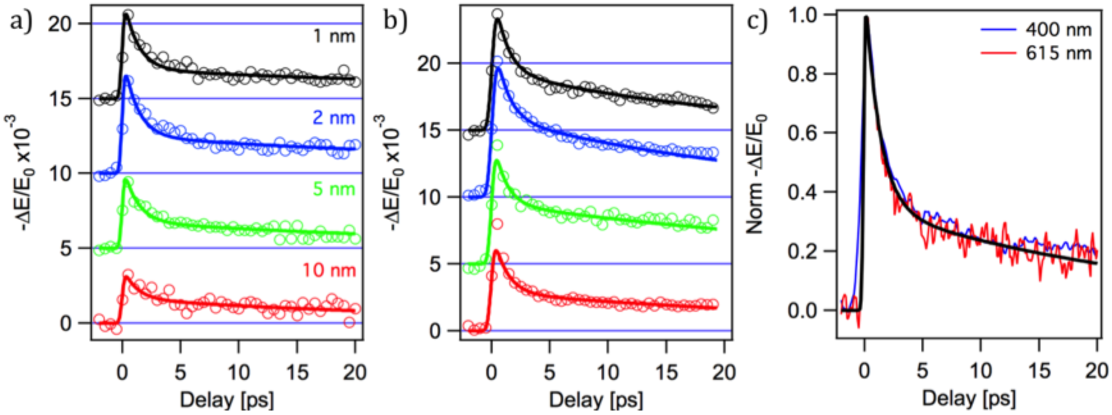


Figure 3. TRTS conductivity dynamics in ZnPc:C_{60} multilayered films shown as a function of layer thickness for (a) 615 nm excitation and (b) 400 nm excitation. (c) Comparison between the TRTS conductivity dynamics resulting from 400 nm (blue) and 615 nm (red) excitation in ZnPc:C_{60} blends. Solid lines are fits to the data.[27]

The photo-induced conductivity depends on the layer thickness for the nanoscale multilayered films. This is most easily observed for 615 nm excitation, which is primarily absorbed by the ZnPc, Figure 3a. Here, the peak photoinduced conductivity increases as the layer thickness decreases, however the conductivity decay rate is independent of thickness.

This is also true when exciting the ZnPc:C_{60} multilayered films with 400 nm light, Figure 3b, however there we see an additional short-lived peak. This peak matches the C_{60} autoionization dynamics and becomes more pronounced for thicker layers, indicating it comes from regions of bulk C_{60}.

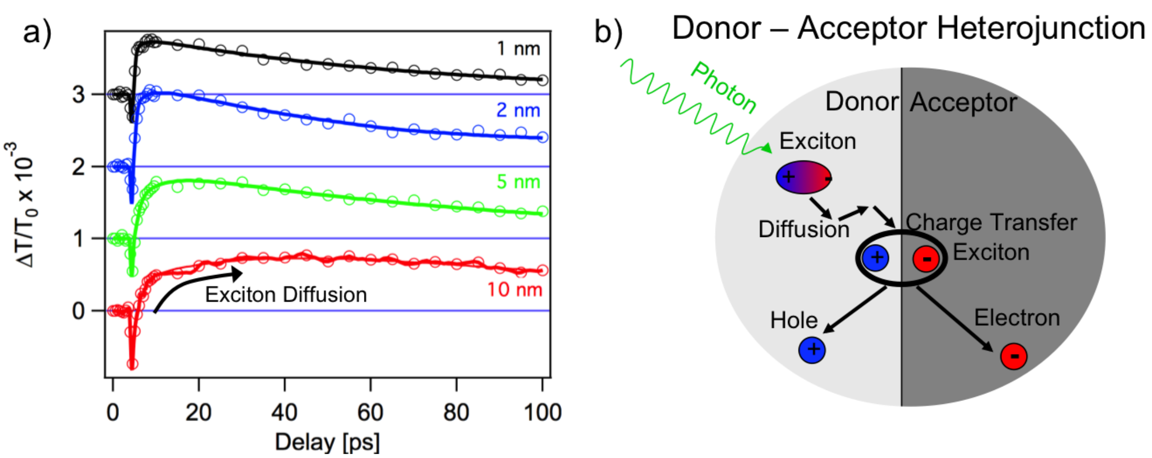


Figure 4. (a) ZnPc Ground state bleach dynamics in ZnPc:C_{60} multilayered films probed at 675 nm after 387.5 nm excitation as a function of layer thickness. Solid lines are Monte Carlo simulations of exciton diffusion in C_{60}. (b) Schematic showing the processes of absorption, exciton creation, diffusion, CTE formation that precede charge separation in a donor-acceptor heterojunction.

As we have seen that the photoconductivity arises from ultrafast charge transfer between donor and acceptor, we can infer that it is dominated by the donor:acceptor interface. Excitation of a donor or acceptor molecule within a layer requires exciton migration to the interface prior to charge transfer. We can estimate the exciton diffusion time by monitoring the ZnPc ground-state bleach (GSB) via TA after excitation at 387.5 nm, Figure 4. At this wavelength, most of the light is absorbed by C_{60}. For the thickest layers, the GSB peak is delayed by 10s of picoseconds. Monte Carlo simulation of hopping between neighboring C_{60} molecules in a face centered cubic lattice with 1.4 nm lattice spacing and unity probability of charge transfer at the ZnPc:C_{60} interface yield a hopping rate of 2.5 THz for all layer thicknesses.[21] This corresponds to an exciton diffusion length of 10 nm, which is typical for an organic semiconductor. This estimate does not include long lived triplet states. We can therefore conclude that charge transfer from molecules excited within the bulk of these nanoscale layers does not contribute to the initial photoinduced conductivity transient. This explains the aforementioned dependence of photoinduced conductivity on layer thickness: as the layers become thinner we expect that a greater fraction of excited states to be created closer to the interface where they are able to contribute to charge separation.

Importantly, there appears to be little dependence of the conductivity dynamics on the excitation wavelength. While a direct comparison within the multilayered films is obscured by the C_{60} autoionization peak, it is much more straightforward for the blended architecture. Here, it is clear that the decay dynamics are the same for 400 nm and 615 nm excitation, Figure 3c. When ZnPc is preferentially excited at 615 nm, electrons transfer into a high-lying excited state of C_{60}, resulting in a hot carrier. Similarly, when C_{60} absorbs a 400 nm photon an electron directly excited into such a state, as discussed above for the case of autoionization. In the case of ZnPc:C_{60}, hole transfer into ZnPc occurs prior to electrons thermalizing in C_{60}, giving rise to the observed photoinduced conductivity dynamics. Clearly charge transfer can compete with hot CTE cooling.

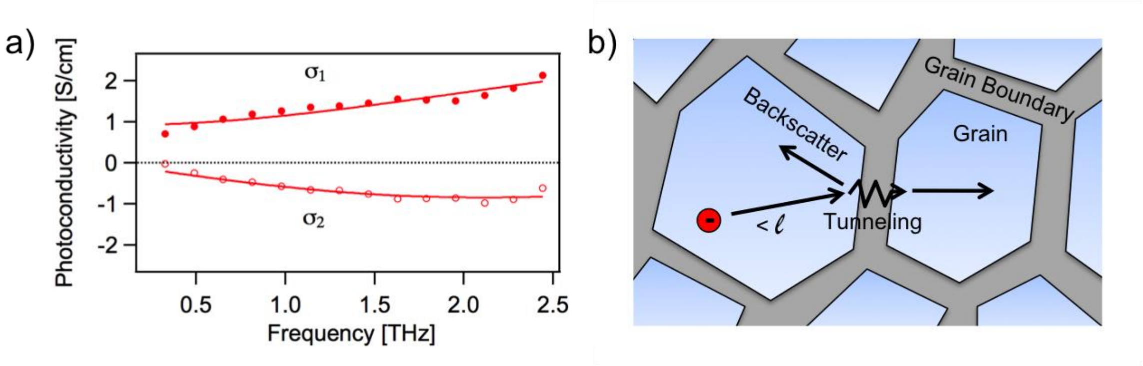


Figure 5. (a) Real (σ_1) and imaginary (σ_2) frequency-dependent conductivity in multilayered ZnPc:C_{60} films with 5 nm layers. The solid lines are fits to the Drude-Smith model. (b) Schematic representation of charge carrier backscattering over distances less than the mean free path length (l), which is described by the Drude-Smith model.

The complex frequency-dependent photoinduced conductivity in ZnPc:C_{60} shows dispersive transport, Figure 5a, where the conductivity increases with frequency. Dispersive transport is characteristic of disordered systems. For Anderson disorder, random defects cause destructive interference among carrier scattering events, leading to localized transport. The effect of nanoscale disorder can be described by the Drude-Smith model,[30] which considers the probability of carrier backscattering from an electronic barrier reached within the charge carrier mean free path length, Figure 5b. Typical barriers include grain boundaries,[31] interfaces, nanoparticle surfaces,[32] or the potential associated with an impurity or defect. This model is typically used to describe the THz conductivity of polycrystalline organic semiconductors,[33] while single crystals show Drude-like transport.[34] Applying such a model to the extracted frequency-dependent conductivity results in a scattering time of 28 ± 2 fs and a backscatter parameter of -0.83 ± 0.01 where -1 represents complete backscatter. These values are comparable to those measured in polycrystalline polymeric systems,[33] and may be dominated by efficient transport in C_{60} layers. No dependence on layer thickness was discernable with the uncertainty of these measurements.

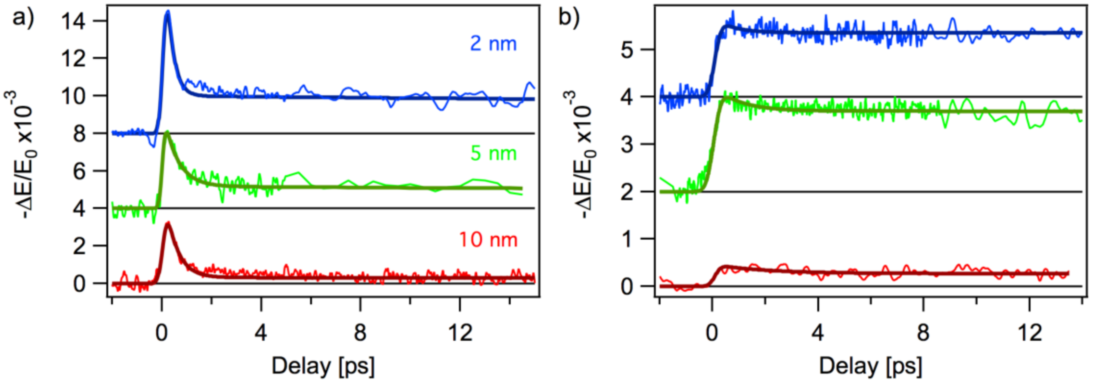


Figure 6. TRTS conductivity dynamics in α-6T:C_{60} multilayer films as a function of layer thickness for (a) 400 nm and (b) 615 nm excitation. Solid lines are fits to the data.

Lastly, we examine the α-6T:C_{60} donor:acceptor system. Photoexcitation with 400 nm light yields qualitatively similar results as those observed in ZnPc:C_{60}, Figure 6a. We observe a short-lived decay to a long-lived residual component. Here, 400 nm light preferentially excites α-6T, and electron transfer into a high-lying C_{60} state results in a hot carrier.

However, photoexcitation at 615 nm yields very different results, Figure 6b. Here, only C_{60} can absorb photons. As we have seen, this photon energy is insufficient for C_{60} alone to generate charge-separated states. However, hole transfer to α-6T yields an equilibrium photoinduced conductivity that persists for > 100 ps. In this case, hole transfer occurs from a "cool" state.[27] This is consistent with emerging evidence that charge separation can occur efficiently even from the lowest ground-state accessible charge transfer states.[35] This demonstrates that charge transfer does not require hot CTEs and instead can occur from thermalized states without a large driving energy.

4. CONCLUSIONS

In summary, we have examined charge transfer in two model molecular systems using time-resolved terahertz spectroscopy and transient absorption spectroscopy. In the case of charge carriers, the former provides the product of the population and mobility, while the later provides only population information. We find, for photon energies above 2.3 eV, that autoionization in C_{60} leads to charge generation. The signature of this process is a sub-picosecond recapture of charges that are unable to escape the electron-hole mutual (Coulombic) attraction. Addition of an electron donor material facilitates charge separation. In the case of ZnPc:C_{60}, the dissociation of charge transfer excitons yields hot charge carriers with excess mobility, which dissipates as charges cool to lower energy levels and localize due to molecular reorganization. This short-lived high mobility may facilitate charge separation in some systems and aid in reducing geminate recombination. This may contribute to reports of increased charge separation yields from hot charge-transfer excitons. In the case of α-6T:C_{60}, we see that charge transfer can occur from states will little excess energy. The observation of charge separation without a significant excess driving energy provides evidence that open circuit voltage losses could be minimized by the use of sufficiently crystalline materials.

REFERENCES

[1] Y. Liu, C.-C. Chen, Z. Hong *et al.*, "Solution-processed small-molcule solar cells: breaking the 10% power conversion efficiency," Sci. Reports, 3, 3356 (2013).

[2] J.-D. Chen, C. Cui, Y.-Q. Li *et al.*, "Single-Junction Polymer Solar Cells Exceeding 10% Power Conversion Efficiency," Adv. Mater., 27, 1035-1041 (2015).

[3] R. Fitzner, E. Mena-Osteritz, A. Mishra *et al.*, "Correlation of π-Conjugated Oligomer Structure with Film Morphology and Organic Solar Cell Performance," J. Amer. Chem. Soc., 134, 11064-11067 (2012).

[4] L. A. Perez, K. W. Chou, J. A. Love *et al.*, "Solvent Additive Effects on Small Molecule Crystallization in Bulk Heterojunction Solar Cells Probed During Spin Casting," Adv. Mater., 25, 6380-6384 (2013).

[5] J. R. Tumbleston, B. A. Collins, L. Yang *et al.*, "The influence of molecular orientation on organic bulk heterojunction solar cells," Nat. Photonics, 8, 385-391 (2014).

[6] D. B. Sulas, K. Yao, J. J. Intemann *et al.*, "Open-Circuit Voltage Losses in Selenium-Substituted Organic Photovoltaic Devices from Increased Density of Charge-Transfer States," Chem. Mater., 27, 6583-6591 (2015).

[7] A. A. Bakulin, A. Rao, V. G. Pavelyev *et al.*, "The Role of Driving Energy and Delocalized States for Charge Separation in Organic Semiconductors," Science, 335, 1340-1344 (2012).

[8] K. Vandewal, S. Albrecht, E. T. Hoke *et al.*, "Efficient charge generation by relaxed charge-transfer states at organic interfaces," Nat. Mater., 13, 63-68 (2014).

[9] K. Vandewal, K. Tvingstedt, A. Gadisa *et al.*, "On the origin of the open-circuit voltage of polymer-fullerene solar cells," Nat. Mater., 8, 904-909 (2009).

[10] G. Grancini, M. Maiuri, D. Fazzi *et al.*, "Hot exciton dissociation in polymer solar cells," Nat. Mater., 12, 29-33 (2013).

[11] N. R. Monohan, K. W. Williams, B. Kumar *et al.*, "Direct Observation of Entropy-Driven Electron-Hole Pair Separation at an Organic Semiconductor Interface," Phys. Rev. Lett., 114, 247003 (2015).

[12] D. C. Coffey, B. W. Larson, A. W. Hains *et al.*, "An Optimal Driving Force for Converting Excitons into Free Carriers in Excitonic Solar Cells," J. Phys. Chem. C, 116, 8916-8923 (2012).

[13] B. Bernardo, D. Cheyns, B. Verreet *et al.*, "Delocalization and dielectric screening of charge transfer states in organic photovoltaic cells," Nat. Commun., 5, 3245 (2014).

[14] K. Cnops, B. P. Rand, D. Cheyns *et al.*, "8.4% efficient fullerene-free organic solar cells exploiting long-range exciton energy transfer," Nat. Commun., 5, 3406 (2014).

[15] R. Ulbricht, E. Hendry, J. Shan *et al.*, "Carrier dynamics in semiconductors studied with time-resolved terahertz spectroscopy," Rev. Mod. Phys., 83, 543 (2011).

[16] P. D. Cunningham, “Accessing Terahertz Complex Conductivity Dynamics in the Time-Domain,” IEEE Trans. THz Sci. Tech., 3, 494-498 (2013).

[17] P. D. Cunningham, L. M. Hayden, H. L. Yip *et al.*, “Charge carrier dynamics in metallated polymers investigated by optical-pump terahertz-probe spectroscopy,” J. Phys. Chem. B, 113, 15427-15432 (2009).

[18] O. Esenturk, J. S. Melinger, P. A. Lane *et al.*, “Relative Photon-to-Carrier Efficincies of Alternating Nanolayers of Zinc Phthalocyanine and C_{60} Films Assessed by Time-Resolved Terahertz Spectroscopy,” J. Phys. Chem. C, 113, 18842-18850 (2009).

[19] S. Kazaoui, R. Ross, and N. Minami, “Intermolecular charge-transfer excitation in C_{60} films: Evidence from luminescence and photoconductivity,” Phys. Rev. B, 52, R11665 (1995).

[20] M. Ichida, A. Nakamura, H. Shinohara *et al.*, “Observation of triplet state of charge-transfer excitons in C_{60} thin film,” Chem. Phys. Lett., 289, 579-585 (1998).

[21] P. A. Lane, P. D. Cunningham, J. S. Melinger *et al.*, “Photoexcitation Dynamics in Films of C_{60} and Zn Phthalocyanine with a Layered Nanostructure,” Phys. Rev. Lett., 108, 077402 (2012).

[22] A. E. Jailaubekov, A. P. Willard, J. R. Tritsch *et al.*, “Hot charge-transfer excitons set the time limit for charge separation at donor/acceptor interfaces in organic photovoltaics,” Nat. Mater., 12, 66-73 (2013).

[23] K. Chen, A. J. Barker, M. E. Reish *et al.*, “Broadband Ultrafast Photoluminescence Spectroscopy Resolves Charge Photogeneration via Delocalized Hot Excitons in Polymer:Fullerene Photovoltaic Blends,” J. Amer. Chem. Soc., 135, 18502-18512 (2013).

[24] E. Hendry, J. M. Schins, L. P. Candeias *et al.*, “Efficiency of Exciton and Charge Carrier Photogeneration in a Semiconducting Plymer,” Phys. Rev. Lett., 92(19), 196601 (2004).

[25] X. He, G. Zhu, G. Yang *et al.*, “Photogenerated Intrinsic Free Carriers in Small-molecule Organic Semiconductors Visualized by Ultrafast Spectroscopy,” Sci. Reports, 5, 17076 (2015).

[26] C. S. j. Ponseca, A. Yartsev, E. Wang *et al.*, “Ultrafast Terahertz Photoconductivity of Bulk Heterojunction Materials Reveals High Carrier Mobility up to Nanosecond Time Scale,” J. Amer. Chem. Soc., 134, 11836-11839 (2012).

[27] P. A. Lane, P. D. Cunningham, J. S. Melinger *et al.*, “Hot Photocarrier Dynamics in Organic Solar Cells,” Nat. Commun., 6, 7558 (2015).

[28] D. G. Cooke, F. C. Krebs, and P. U. Jepsen, “Direct Observation of Sub-100fs Mobile Charge Generation in a Polymer-Fullerene Film,” Phys. Rev. Lett., 108, 056603 (2012).

[29] G. Nan, X. Zhang, and G. Lu, “Do “Hot” Charge-Transfer Excitons Promote Free Carrier Generation in Organic Photovoltaics?,” J. Phys. Chem. C, 119, 15028-15035 (2015).

[30] N. V. Smith, “Classical generalization of the Drude formula for the optical conductivity,” Phys. Rev. B, 64, 155106 (2001).

[31] J. D. Buron, F. Pizzocchero, B. S. Jessen *et al.*, “Electrically Continuous Graphene from Single Crystal Copper Verified by Terahertz Conductance Spectroscopy and Micro Four-Point Probe,” Nano Lett., 14, 6348-6355 (2014).

[32] H. Nemec, P. Kuzel, and V. Sundstrom, “Far-infrared response of free charge carriers localized in semiconductor nanoparticles,” Phys. Rev. B, 79, 115309 (2009).

[33] P. D. Cunningham, and L. M. Hayden, “Carrier dynamics resulting from above and below gap excitation of P3HT and P3HT/PCBM investigated by optical-pump terahertz-probe spectroscopy,” J. Phys. Chem. C, 112, 7928-7935 (2008).

[34] O. Ostroverkhova, D. G. Cooke, S. Shcherbyna *et al.*, “Bandlike transport in pentacene and functionalized pentacene thin films revealed by subpicosecond transient photoconductivity measurements,” Phys. Rev. B, 71, 035204 (2005).

[35] B. R. Gautam, R. Younts, W. Li *et al.*, “Charge Photogeneration in Organic Photovoltaics: Role of Hot versus Cold Charge-Transfer Excitons,” Adv. Energy Mater., 6, 1501032 (2015).

EFFECT OF INTERFACE MOISTURE CONTENT ON THE BOND PERFORMANCE BETWEEN A CONCRETE SUBSTRATE AND A NON-SHRINK CEMENT-BASED GROUT

Igor De la Varga, Ph.D., SES Group & Associates, (202)493-3433, igor.delavarga.ctr@dot.gov
José F. Muñoz, Ph.D., SES Group & Associates, (202)493-3159, jose.munoz.ctr@dot.gov
Dale P. Bentz, National Institute of Standards and Technology, (301)975-5865, dale.bentz@nist.gov
Benjamin A. Graybeal, Ph.D., P.E., Federal Highway Administration, (202)493-3122, benjamin.graybeal@dot.gov

ABSTRACT

An increasing amount of bridge construction in the U.S. is completed through the use of prefabricated bridge elements (PBE), commonly relying on field-cast grout-type materials to complete the connections between precast concrete elements. The interface bond between the grout and the substrate concrete can be a key factor in the long-term durability of the structural system. This paper evaluates bond performance of a non-shrink cementitious grout, and examines how the supply of extra moisture at the grout-concrete interface affects the bond strength. The results show increased bond strength when supplemental moisture is provided to the substrate interface.

INTRODUCTION

The connection of prefabricated concrete elements using field-cast "non-shrink" cementitious grouts is a common practice in accelerated bridge construction (ABC) projects (1). The grout material should have sufficient strength and should offer good bond to the concrete element in order to insure adequate stress transfer not only during loading of the structure, but also during expansion and/or contraction of the newly placed grout material. However, recent studies have reported dimensional stability concerns (primarily shrinkage) in these grout materials (2), which could lead not only to durability problems of the grout material but also to the reduction of the bond between the grout and the prefabricated concrete element.

Many are the variables that affect the bond performance of a cementitious material (e.g., grout) when it is placed in contact with another cementitious material (e.g., concrete substrate) (3). One of them is the provision of extra moisture at the concrete surface before the pour of the new material. This is done with the goal of achieving a saturated-surface dry (SSD) condition on the substrate surface. It is hypothesized that the presence of this extra moisture to achieve an SSD condition will reduce the moisture transfer that might occur from the fresh material into the concrete substrate, thus allowing the fresh material to use of all its available mixing water for a better hydration, as well as reducing shrinkage derived from the water migration. Shrinkage in the freshly poured material will not only increase the "gap" between the two materials, but it will also induce shrinkage stresses at the interface, typically causing microcracking. Since this practice of achieving an SSD condition by adding extra moisture has become common in the construction industry (especially in repair applications), this paper focuses on evaluating the effect that the supply of that extra moisture at the grout-concrete interface has on the bond performance.

EXPERIMENTAL

The bond assessment was performed using the ASTM C1583 test method ("pull-off" test method) on a grout-concrete slab (Figure 1). The slab dimensions were 36 in x 36 in x 4 in (914 mm x 914 mm x 102 mm) with a 2-inch (50-mm) thick overlay of a non-shrink cementitious grout. Prior to the grout pour, the top surface of the concrete slab was pressure washed at 24 h after casting in order to create an exposed aggregate interface, achieved by using a commercially available in-form paint-like retarder agent. The grout was cured for 2 d or 14 d prior to execution of the bond tests. The results are then presented as "2-d" or "14-d" bond strength which refers to the age of the grout when the bond test was performed.

de la Varga, Igor; Munoz, Jose; Bentz, Dale; Graybeal, Benjamin.
"Effect of the Interface Moisture Content on the Bond Performance between a Concrete Substrate and a Non-Shrink Cement-Based Grout."
Paper presented at the National Accelerated Bridge Construction Conference, Miami, FL, Dec 7-Dec 8, 2015.

In this study, the moisture is provided by either saturating the concrete surface during the 24 h that precede the casting of the grout, so that an SSD condition is achieved, or by means of internal curing (IC) through the use of pre-wetted light-weight aggregates (LWA) being included in the grout material. The LWA used had a specific gravity value of 1.57, and a water absorption value of 16.6 %. The amount of LWA added was 23 % of the solid content, by mass. Water from the LWA will be released at the appropriate time (typically after set), and will theoretically migrate to the regions where water is demanded (e.g., grout-concrete interface). The provision of IC using LWA, besides providing extra moisture at the interface, will also reduce shrinkage of the grout and improve grout curing conditions (4). Finally, images taken from an environmental scanning electron microscope (SEM) will be utilized in order to observe if the extra moisture provided has an influence on the microstructural features (e.g., main hydration products formed) of the grout-concrete interface.

RESULTS

Figure 1 shows the 2-d and 14-d pull-off results. All the specimens failed at the grout-concrete interface (except for the tensile results in which the specimens failed within the grout material). Results labelled as “control” correspond to the specimens where no moisture was added (i.e., drying conditions at a temperature of 23 °C ± 1 °C and a relative humidity of 50 % ± 5 %). “SSD” and “IC” correspond to the specimens where additional moisture was provided via 24-h water saturation or IC, respectively. The pull-off tensile strength of the grout material for all the specimens was added for reference purposes. As can be observed, the bond strength increases over time, since the 14-d strength is (in all cases) larger than at 2 d. The bond strength of the SSD specimens is about 45 % and 17 % higher than that of the control at 2 d and 14 d, respectively. As for the IC specimens, while the 2-d bond strength is about 18 % higher than the control, the bond strength obtained at 14 d was not significantly different. One aspect to point out about the IC samples is that they showed a larger number of air pockets (e.g., large porosity) at the interface. This might be attributed to the fact that the LWA needed to provide IC is added to the grout material, reducing its paste content per unit volume and slightly changing the rheology by making the material less fluid. It is conjectured that this could have an impact on the bond strength by reducing the contact area. The same effect was also observed at 2 d, although the bond strength obtained was slightly larger (perhaps, other variables such as the increased degree of hydration due to the extra moisture have more effect on the bond strength at this age). The tensile strength is always larger than that of the interface failure, confirming that the weakest region is located at the grout-concrete interface, at least up to 14 d of hydration (noting that the 2-d IC tensile strength could not be measured).

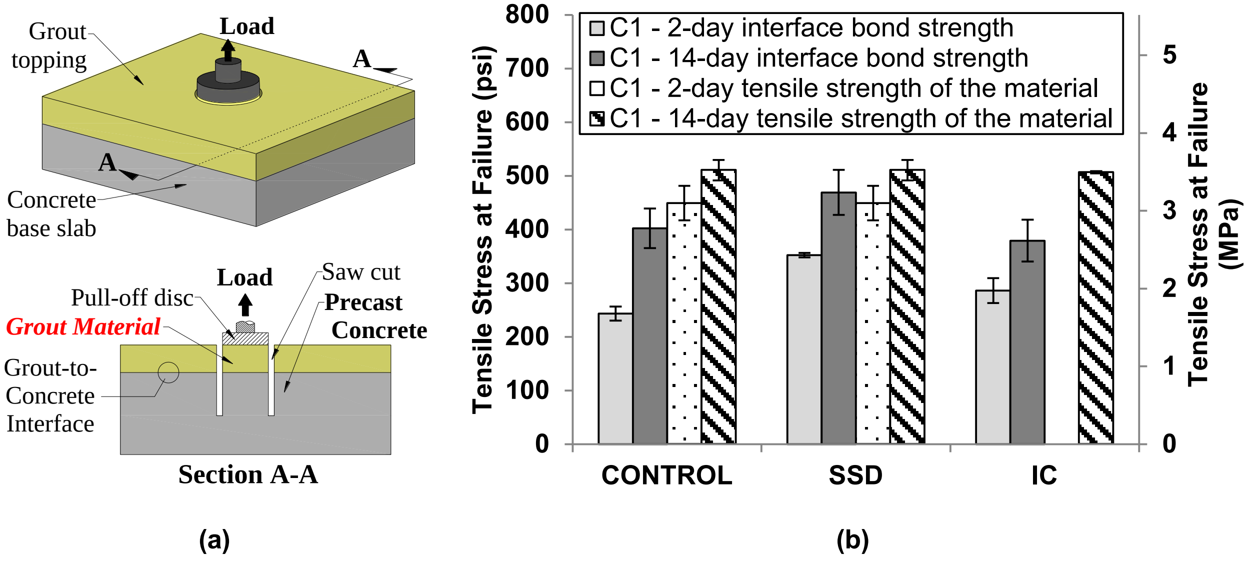


Figure 1. (a) Illustration of the pull-off test on the grout-concrete slab via ASTM C1583, (b) 2-d and 14-d pull-off bond strength for the different interface moisture conditions. (Error bars represent ± one standard deviation from the average of four samples)

DISCUSSION AND CONCLUSIONS

In an attempt to explain the bond strength results, SEM images were collected from the grout side of the interface in each of the specimens studied: control, SSD, and IC. A clear difference on the type of crystals formed was observed between the control and the specimens with extra moisture (SSD and IC). While the microstructure on the control specimen was dominated by the presence of large blade-shaped crystals randomly oriented, both SSD and IC specimens showed a microstructure dominated by the presence of denser 'equant' crystals, with a morphology closer to cubical and thick needle shapes (Figure 2b, 2c). The earlier formation of this type of crystal was promoted by the presence of extra moisture at the interface. Eventually, the bladed-shaped crystals of the control specimen will also transform into the denser equant crystals (as observed in the 14-d SEM micrographs, although not shown in this paper). The presence of extra moisture accelerates this transformation. It is then conjectured that the equant shape of those crystals increases the contact area between the grout and the concrete, compared to that of the blade-shaped crystals (that is, a more interpenetrating contact type).

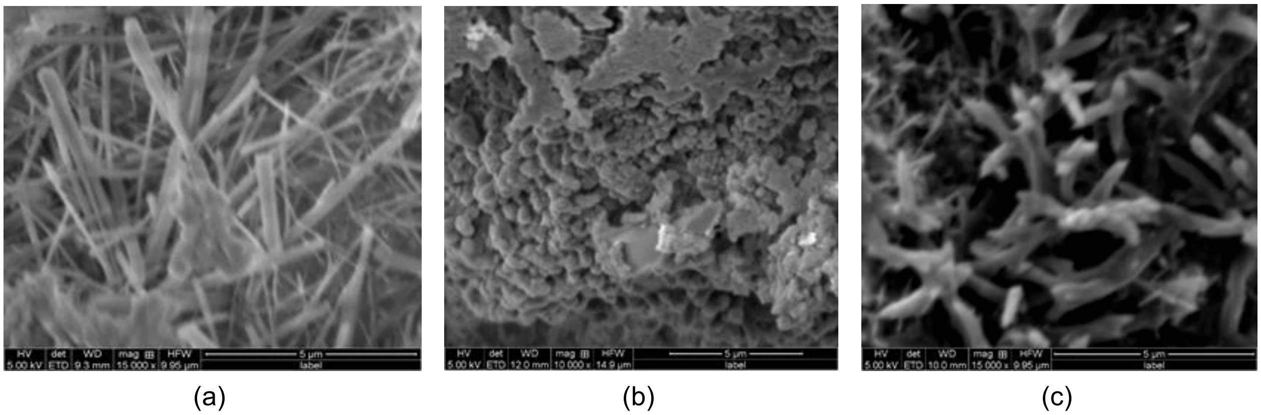


Figure 2. 2-d SEM micrographs of the control fractured sample at the grout side of the interface: (a) control, (b) SSD, (c) IC.

In conclusion, the presence of extra moisture (i.e., SSD condition) at the concrete surface changes the type of microstructure present at the interface, increasing the bond strength at the grout-concrete interface.

ACKNOWLEDGMENTS

The authors would like to thank Daniel Balcha of SES Group & Associates for his technical assistance and Paul Stutzman from NIST for his valuable comments. The research which is the subject of this document was funded by the U.S. Federal Highway Administration. This support is gratefully acknowledged. The publication of this report does not necessarily indicate approval or endorsement of the findings, opinions, conclusions, or recommendations either inferred or specifically expressed herein by the Federal Highway Administration, the National Institute of Standards and Technology, or the United States Government.

REFERENCES

1. Culmo, M. P. (2009). Connection details for prefabricated bridge elements and systems (No. FHWA-IF-09-010).
2. De la Varga I, Graybeal B (2014). "Dimensional stability of grout-type materials used as connections between prefabricated concrete elements". *Journal of Materials in Civil Engineering*, 2014; DOI: 10.1061/(ASCE)MT.1943-5533.0001212
3. Silfwerbrand, J., & Beushausen, H. (2005). Bonded Concrete Overlays: Bond Strength Issues. In *International Conference on Concrete Repair, Rehabilitation and Retrofitting* (pp. 19-21).
4. Bentz, D. P., & Weiss, W. J. (2011). Internal curing: A 2010 state-of-the-art review. US Department of Commerce, National Institute of Standards and Technology.

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2015) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

Complex Adaptive Systems, Publication 5
Cihan H. Dagli, Editor in Chief
Conference Organized by Missouri University of Science and Technology
2015-San Jose, CA

Using Semantic Web Technologies for Integrating Domain-specific Modeling and Analytical Tools

Mark R. Blackburn[a]*, Peter O. Denno[b]

[a]Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ, 07030, USA
[b]National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD, 20899-8260, USA

Abstract

This paper discusses the potential advantages and pitfalls of using semantic web technologies for representing and integrating modeling and analysis tools. Analytical tools are often not designed to be integrated with information sources and general-purpose modeling tools and often do not support detection of problems across domains. Additionally, these modeling tools may not capture and represent explicitly the information needed to leverage the capabilities of analysis tools. The method described uses semantic web technology as the integrating mechanism between domain specific modeling (DSM) tools and analytical tools. We describe a method and tool set for representing the analytical knowledge through semantic web ontologies that map between the metamodels of both the DSM and analytical tools. We compare an earlier tool-chain prototype with a significantly revised prototype to reflect on the benefits from using semantic web technologies as an integrating mechanism. A potential advantage is the ability to explicitly and transparently represent the relationships between modeling and analytical tools.

© 2015 The Authors. Published by Elsevier B.V.

Peer-review under responsibility of scientific committee of Missouri University of Science and Technology.

Keywords: domain specific modeling; cyber physical systems; metamodeling; ontologies; semantic web; model-centric engineering;

1. Introduction

The pervasive use of networking, sensors and information technologies to create smart or intelligent systems offers increased effectiveness, productivity, safety, and enables increased functionality in smart manufacturing and more generally Cyber Physical Systems (CPS). Model-centric engineering (MCE) is increasing in use to deal with

* Corresponding author. Tel.: 1-561-637-3452.
E-mail address: mark.blackburn@stevens.edu

1877-0509 © 2015 The Authors. Published by Elsevier B.V.

Peer-review under responsibility of scientific committee of Missouri University of Science and Technology. This work was partially funded by NIST through contract SB1341-12-CQ-0011 to Dakota Consulting, Inc..

the increased complexity in analyzing both the problem and solutions for CPS. MCE is an overarching digital approach for integrating different model types and tools for simulations and analysis of systems and components at different levels of abstraction and fidelity across disciplines throughout the lifecycle[1]. MCE technologies enable more automation and efficiencies, however there is still a lack of cross-domain model interoperability, consistency, and limitations transforming models with the required semantic precision to provide accurate information for some required analysis.

In the context of this paper, we are concerned with disparate modeling viewpoints and the associated analytical knowledge that is required to leverage analysis tools to support decision making about integration of computationally-enabled equipment and functions of a smart-manufacturing system. These viewpoints are modeled using DSMs that can require cross-domain analyses for detecting anomalies and incompatibilities that may arise when new capabilities are introduced into systems. We extend a prototype used in prior research[2] because that work documents the analytical results and benefits of integrating DSM tools with analysis tools[†]. The prototype discussed herein keeps fixed the DSM metamodel, application models and analysis tool capabilities in order to compare and contrast the use of semantic web technologies as an analytical knowledge representation and integrating mechanism. We focus on declarative and traceable means to compose information into analytical models.

In the field of design and engineering, knowledge can be classified along several dimensions: formal versus tacit, product versus process, and compiled versus dynamic[3]. Sowa describes knowledge representation as a multidisciplinary subject that combines techniques from logic, ontology, and computation[4]. Ontologies represent a possible way to generate a more flexible data model integrating disparate knowledge domains[5]. We want to make various aspects of these classes of engineering knowledge explicit by formalizing unstructured and tacit knowledge. We believe logic, ontology, and computation are key aspects for formalizing different types of knowledge for cross-domain and multidisciplinary analyses.

The semantic web technologies are based on a standard suite of languages, models, and tools that are suited to knowledge representation. Fig. 1 provides a perspective on the semantic web technology stack, which includes eXtended Markup Language (XML)[6], Resource Description Framework (RDF)[7] and RDF Schema (RDFS)[8], Web Ontology Language (OWL)[9], querying language (SPARQL)[10], and others. RDF can describe instances of ontologies. RDFS extends RDF and provides primitives such as Class, subClassOf, and subPropertyOf. The semantic web technologies were created to extend the current Internet allowing combinations of metadata, structure, and various technologies enabling machines to derive meaning from information, both assisting and reducing human intervention. This technology is generally applicable beyond the original intent, as we will discuss in this paper.

The technology layers of the semantic web support different levels of abstractions. OWL has found acceptance as a standard notation for knowledge representation. OWL-enabled modeling tools are available from multiple providers, as well as supporting assets such as reasoners and application-programming-interface libraries. OWL has been applied to diverse projects in a wide array of fields[11]. OWL was developed from the beginning based on formal logical principles; it provides strong support for verification of consistency and satisfiability, extraction of entailments, and conjunctive query answering. This emphasis on formal logic counterbalances the absence of any graphical-notation conventions in the OWL standards[12]. Some researchers have attempted to use RDF without OWL for related model-based analysis effort such as requirement representation and trade space analysis[11], however these attempts have required using code in the transformation to perform needed functions such as inferencing, which is supported more directly by OWL-capable tools.

We focus on the use of the semantic web technologies at the ontology and reasoning layer to represent analytical knowledge as reflected in Fig. 1. The notion of a metamodel of a DSM is strongly related to the notion of a domain ontology[13], because both are an abstraction of a conceptualization[14]. Ontologies in OWL are associated with metamodels of a DSM and also map to the metamodels of analysis tools. Our interest is in the methods of

[†] Certain commercial software products are identified in this paper. These products were used only for demonstration purposes. This use does not imply approval or endorsement by NIST, nor does it imply these products are necessarily the best available for the purpose.

representing the analytical knowledge to take advantage of a standards-based approach to knowledge representation, transformation and formal analysis. The transformations are applied to specific instances of information derived from models as subject, predicate and object using RDF triples that are compliant with their respective ontology.

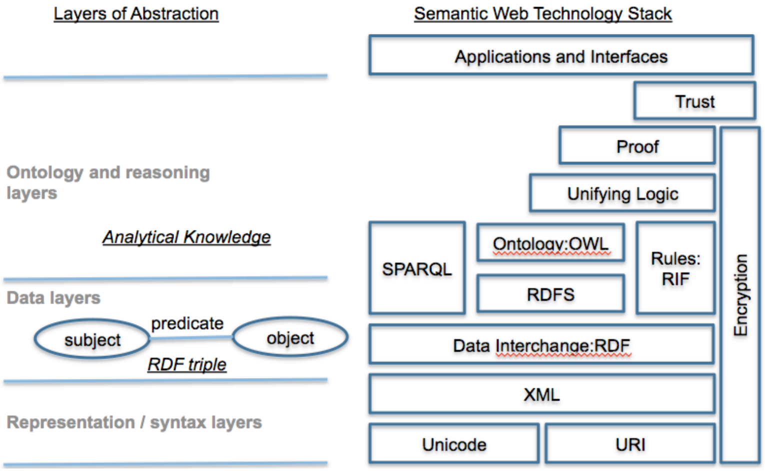


Fig. 1. Semantic Web Technologies related to Layers of Abstraction.

2. Context

There are many stakeholders involved in various roles that contribute to both the problem formulation and solution of a CPS. These stakeholders have differing concerns related to trade space, design, integration, safety, operations, etc. A viewpoint establishes the purpose and audience for a representation of a system[15]. Viewpoints relevant to production include representations of schedules, process plans, inspection results, inventory, unit process descriptions and equipment datasheets. Each of them has some type of conceptualization of how their view applies to the overall problem formulation and process as reflected in Fig. 2. The conceptualizations of these views can be represented in a semantically precise way using ontologies[16].

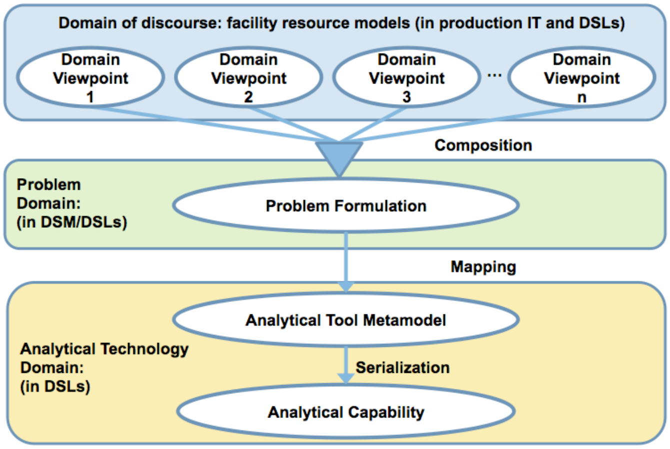

Domain of discourse: facility resource models (in production IT and DSLs)
Domain Viewpoint 1
Domain Viewpoint 2
Domain Viewpoint 3
...
Domain Viewpoint n
Composition
Problem Domain: (in DSM/DSLs)
Problem Formulation
Mapping
Analytical Tool Metamodel
Analytical Technology Domain: (in DSLs)
Serialization
Analytical Capability

Fig. 2. Transforming Views of the Problem in order to Leverage Analytical Capabilities for a Specific Objective.

By expressing the problem formulation metamodel as an OWL ontology, we enable three capabilities that are not easily achieved by other means. First, the problem formulation ontology represents a composition of more fundamental viewpoints that are oftentimes provided without interrelation in the domain of discourse. The problem formulation ontology enables an analysis of the compositionality of those views. For example, the interconnection of component equipment may be provided by a piping and instrumentation diagrams (P&ID), whereas a behavioral viewpoint is provided by a mechanical control view. It is possible that some entailments of the composition of viewpoints are incompatible. For example, the controls view may suggest that a component valve provides a regulating function, whereas the equipment view indicates that the same valve is only intended to provide safety pressure relief.

Second, OWL axioms may be applied against the problem formulation ontology to ensure that individual viewpoints are well-formed. For example, pipes, elements of the P&ID view, may be constrained to have connections on two ends. This example illustrates one of the shortcomings in our first prototype[2]; the DSM system captured the needs for these types of constraints, however, it was not visible to the analytical tool through the model transformation.

Third, the problem formulation ontology enables traces to requirements. Tracing requirements is problematic because design tools oftentimes do not enable annotation of requirements on design elements, or such annotation is only possible on abstract system viewpoints, such as those provided by SysML[17]. The openness of ontology-based development enables requirements to be superimposed ad hoc over existing viewpoints.

The use of an ontology for the problem formulation does, however, presents its own challenges. Foremost among these is that it does not provide straightforward means to organize mapping to the analytical tool metamodel. As suggested in our earlier work[18] analytical metamodels emphasize structural containment and part-whole relationships because it is commonplace for software to require syntactically structured input.

3. Objective and Approach

We significantly modified the tool chain used in prior efforts,[2] as shown in Fig. 3. The context of that research focused on virtual design and verification of industrial process plants' designs. The prototype used DSMs and DSLs of a system design, and provided examples of how the integration with formal methods can identify defects in the design, and automatically generates test vectors with requirement-to-test traceability. The project research involved three main roles: 1) developing the DSM metamodel for integrated system designs, 2) creating application-specific models, using two graphical DSLs, and 3) producing the generator required to demonstrate analysis and test generation. The elements of the prior prototype are shown as shaded elements such as the DSM (MetaEdit+[19]) metamodels, associated application models and T-VEC[20] analysis, test vector generation and requirement traceability capabilities. These elements remain fixed in the updated prototype in order to formulate a comparison of the potential advantages and pitfalls of the new approach over the prior approach.

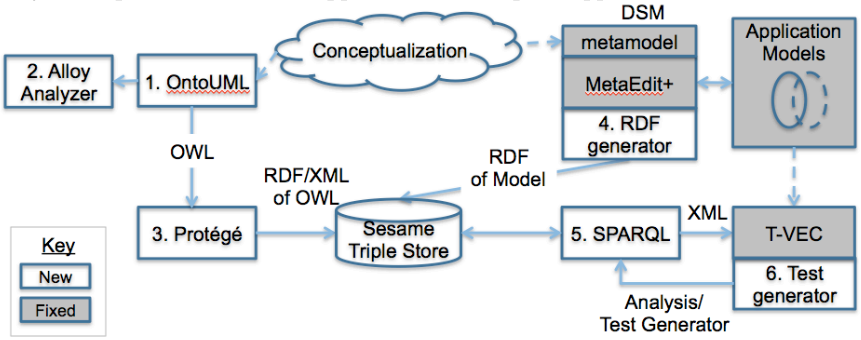


Fig. 3. Ontology, Domain Specific Modeling, Analysis and Semantic Web Prototype

As detailed below, the modifications to the prototype are reflected by the unshaded elements in Fig. 3. These elements provide the new functionality of the prototype; these are used to model and analyze ontologies used by the semantic web technologies and for representing analytical knowledge to transform model instances into representations required by the analysis tools (i.e., Alloy Analyzer[21], T-VEC). The functions performed by the new elements in Fig. 3 are labeled below.

1. We created the initial ontology with Protégé, an open-source ontology editor and framework[22], but adopted a more rigorous method for developing a domain ontology representation, in which we used a lightweight modeling languages and tool, OntoUML lightweight editor (OLED)[23]. We modeled our conceptualization of the P&ID domain using OLED, which also produces an OWL ontology in XML. Having a precise representation of a given conceptualization becomes even more valuable when we want to integrate different independently-developed models or systems based on those models[24], as reflected by the problem formulation discussed in Section 2.

2. OLED also produces an Alloy specification[21]. The Alloy Analyzer is a solver that checks an Alloy specification for well-formedness properties and satisfiability of constraints. The Alloy Analyzer also produces visualizations of possible instances derived from the modeled ontology. This has the benefit to allow the ontology modeler and domain subject matter experts a way to visualize possible instances from the ontoUML model and provides a type of early model validation of the modeled ontology.

3. We use Protégé to convert OWL to RDF/XML for loading into an inferencing-enabled Sesame triple store.

MetaEdit+ is a tool that provides capabilities to represent a conceptualization as a metamodel and allow users to construct specific application models (instances) that are compliant with the metamodel. MetaEdit+ provides a template-based generator capability to support transformations of application models into artifacts such as documents, code, or other types of language generation. In our prior effort[2], we used the generator and some additional software to perform the application model transformations into T-VEC specifications; that research was focused on integrating DSMs with formal method tools like T-VEC. T-VEC is a theorem prover that we used to prove different types of properties (e.g., flow, pressure) were valid in the application model. T-VEC also generates test vectors with requirement-to-test traceability; these same capabilities are performed in the new version of the tools.

4. In the new prototype, we created a different MetaEdit+ generator (RDF generator) that produces RDF representations of the application models. The generator was significantly simpler (i.e., about one third the code size of the prior version). We can demonstrate that these models are compliant with the OWL ontology through formal logics; these kinds of capabilities are well documented[12] and complements our approach, because the models have the necessary formalization in OWL and RDF.

5. We created SPARQL queries to extract information and serialize it into the XML-based language of T-VEC. This was also straightforward. eliminating the generator code we used in the earlier prototype. The current version uses SPARQL queries through an application programming interface to the triple store, which made the serialization of the XML to T-VEC easier to do. These same SPARQL queries can be executed from a web browser.

6. The outputs of the analysis and test vector generation processes are loaded back into the triple store repository. Users can use web browsers to perform SPARQL queries directly to examine the results or through application program libraries in several different languages. Some researchers have created natural languages interfaces to further simplify the interface and raise the level of abstraction for presenting the semantic web information to subject matter experts in the domain[25].

4. Conclusions

We describe the approach to transform DSMs through semantic web technologies and have been successful in demonstrating a new variant of our tool set. The new approach uses domain conceptualization, both in terms of metamodels and ontologies providing a way to cross check between representations to ensure semantic consistency. This not only improves on the prior approach, but provides for a more comprehensive and systematic approach for characterizing the domains associated with the problem formulation ontology concept. In addition, we believe that the early validation capabilities provided through model satisfiability checking and visualization of specific model instances using tools like the Allow Analyzer are valuable for subject matter experts across the related domains.

The new approach simplifies the DSM generator signficantly. It does require more effort in developing the ontology, but that has value as described previously. In addition, the ontology, if defined appropriately can leverage inferencing in the triple store, which can only be done from either RDFS or OWL. The inferencing creates RDF in the triple store for associations (e.g., class, subclass) derived from the model. These types of associates were previously produced through code in the generator of the early prototype as they are required for the model transformation into T-VEC. In addition, the new serialization using SPARQL, which is also straightforward as all of the needed information is in the triple store, and again requires significantly less code. SPARQL is a relatively simple open, standard-based language. Its simplicity facilitates verification. These results derived through the application of semantic web technologies reflect well on our desire to have more transparency of the analytical knowledge, in this case focused mostly on the model transformations.

The methodology underlying the ontoUML approach adds methodological rigor, which like any methodology involves learning, but the rigor and associated analysis and visualization tools pay off through model validation. This approach leads also to the need for methodological rigor in developing of the ontology as the users need to understand how the ontology generation process works (e.g., the generation of namespaces in the RDF).

The new aspects of the approach are open and standards-based that address some of the needs for semantically precise representation of MCE. Equally important is that the transformation medium is potentially tool agnostic, which can have significant potential benefits on coordinating efforts between companies that don't use the same tooling. A tool agnostic approach is desirable in the acquisition of complex systems. As we move into a world where we need to share more information digitally, imposing any particular set of tools on the contractors and developers of these systems is problematic. Not only is this information important for early conceptualization and design, but the availability for digitally precise and semantically rich information is more important in manufacturing, operations and sustainment.[26]

References

1. Blackburn, M., R. Cloutier, G. Witus, E. Hole, M. Bone, Transforming System Engineering through Model-Centric Engineering, SERC-2014-TR-044-2, January, 2015.

2. Blackburn, M., P. Denno, Virtual Design and Verification of Cyber-physical Systems: Industrial Process Plant Design, Conference on Systems Engineering Research, March, 2014; http://dx.doi.org/10.1016/j.procs.2014.03.006.

3. Chandrasegaran, Senthil K., Karthik Ramani, Ram D. Sriram, Imré Horváth, Alain Bernard, Ramy F. Harik, and Wei Gao. "The Evolution, Challenges, and Future of Knowledge Representation in Product Design Systems." Computer-Aided Design 45, no. 2, February 2013.

4. Sowa J. Knowledge representation and reasoning: logical, philosophical, and computational foundations. Brooks/Cole; 2000.

5. Terkaj, W., Pedrielli, G., & Sacco, M. (2012). Virtual Factory Data Model. 7th International Conference on Formal Ontology in Information Systems (FOIS 2012). Graz: IOS Press.

6. Object Management Group, XML Metadata Interchange (XMI), Version, 2.4.2, April 2014, http://www.omg.org/spec/XMI/2.4.2.

7. RDF – Resource Description Framework (RDF): Concepts and Abstract Syntax, W3C Recommendation, 10 February 2004, http://www.w3.org/TR/rdf-concepts/.

8 World Wide Web Consortium. RDF Vocabulary Description Language 1.0: RDF Schema. http://www. w3.org/TR/rdf-schema/, February 2004.

9. World Wide Web Consortium. OWL 2 Web Ontology Language Document Overview. 2009. Available from: http://www.w3.org/TR/2009/REC-owl2-overview-20091027/.

10. SPIN – SPARQL Inferencing Notation: Overview and Motivation, W3C Member Submission, 22 February 2011, http://www.w3.org/Submission/spin-overview/.

11. Nassar, Nefretiti, and Mark Austin. "Model-Based Systems Engineering Design and Trade-Off Analysis with RDF Graphs." Procedia Computer Science 16 (2013): 216–25. doi:10.1016/j.procs.2013.01.023.

12. J. Steven Jenkins, Nicolas F. Rouquette, Semantically-Rigorous Systems Engineering Modeling Using SysML and OWL, Jet Propulsion Laboratory, California Institute of Technology, 2012.

13. Bézivin, J. On the unification power of models. Software and System Modeling, 4(2):171–188, May 2005.

14. Guizzardi, G. "Ontological Foundations for Structural Conceptual Models", Telematica Instituut Fundamental Research Series no. 15, Universal Press, The Netherlands, 2005, ISBN 90-75176-81-3.

15. ISO/IEC 42010:2007, Systems and Software Engineering -- Architecture Description, 2007.

16. Gruber, Thomas R. "Toward Principles for the Design of Ontologies Used for Knowledge Sharing." Int. J. Hum.-Comput. Stud. 43, no. 5–6 (December 1995): 907–28. doi:10.1006/ijhc.1995.1081.

17. OMG System Modeling Language, See http://www.omgsysml.org.

18. Denno, P. O., D. B. Kim, Integrating views of properties in models of unit manufacturing processes, National Institute of Standards and Technology, December 2014.
19. MetaEdit+ Tool Suite, http://www.metacase.com/.
20. T-Vec Tool Suite, http://www.t-vec.com/.
21. Alloy, http://alloy.mit.edu/alloy/.
22. Protégé, http://protege.stanford.edu/.
23. OntoUML lightweight editor , https://code.google.com/p/ontouml-lightweight-editor/
24. Guizzardi, G. "The Role of Foundational Ontologies for Conceptual Modeling and Domain Ontology Representation," 17–25. IEEE, 2006.5doi:10.1109/DBIS.2006.1678468.
25. Sukys, A., Lina Nemuraite, Bronius Paradauskas, Edvinas Sinkevicius, Transformation Framework for SBVR based Semantic Queries in Business Information Systems, The Second International Conference on Business Intelligence and Technology, 2012.
26. Witherell, Paul, Boonserm Kulvatunyou, and Sudarsan Rachuri. "Towards the Synthesis of Product Knowledge Across the Lifecycle," V012T13A071. ASME, 2013. doi:10.1115/IMECE2013-65220.

OPTIMIZED AIR-TO-REFRIGERANT HEAT EXCHANGER WITH LOW-GWP REFRIGERANTS

Honghuyun Cho[(a)], Piotr A. Domanski[(b)]
[(a)]Chosun University
Gwangju, 501-753, S. Korea, hhcho@chosun.ac.kr
[(b)]National Institute of Standards and Technology
Gaithersburg, MD 20899-8631, USA, piotr.domanski@nist.gov

ABSTRACT

This paper presents an analytical evaluation of the performance of low-GWP refrigerants in a finned-tube evaporator used for residential cooling applications. The study employed an evolutionary-computation optimization module to examine the effect of a refrigerant circuitry design on performance of twelve alternative refrigerants for R22 and R410A. The study showed that high-pressure fluids benefited most from refrigerant circuitry optimization, with R744 achieving a capacity increase of over 13 %. Among lower-pressure fluids, the capacity of an R717 evaporator increased by over 10 %. The effect of optimized refrigerant circuitries on the system performance was estimated. The results show that zeotropic blends with a large temperature glide are particularly sensitive to the refrigerant circuitry and may suffer significant performance degradation in heat exchangers with improper design.

Keywords: air conditioning, evaporator, global warming potential, optimization, refrigerants

1. INTRODUCTION

Concerns about climate change, and the recent (EU, 2014) and anticipated regulations phasing down refrigerants with a high global warming potential (GWP), have prompted numerous studies evaluating the performance of low-GWP refrigerants in air-conditioning and refrigeration equipment. Initial performance evaluations typically rely on simple theoretical simulations, which are based on thermodynamic properties alone. The next step often involves laboratory tests in a system that was originally developed for the refrigerant planned to be phased out. While laboratory tests provide the 'most trusted' information about performance of a refrigerant in a given system, it is recognized that tests of a new refrigerant in a system optimized for a different refrigerant (referred to as 'drop-in' tests) do not show the performance potential of the new fluid. 'Soft-optimization', which includes adjustment of the refrigerant charge and expansion device, is typically implemented in drop-in tests; however, optimization of the compressor and refrigerant circuitry in the evaporator and condenser is also needed for fair refrigerant evaluation (Abdelaziz et al., 2015). In this paper we discuss the effect of refrigerant circuitry on the evaporator performance with natural and fluorinated alternatives for R22 and R410A. We applied an evolutionary computation-based optimization module to design refrigerant circuitries for candidate refrigerants and compared the optimized performance in the evaporator with that using the original circuitry.

2. REFRIGERANTS

We considered six R22 alternatives and six R410A alternatives (Table 1). We assigned the alternatives to these two groups based on the pressure of these refrigerants while operating in an air conditioner. The 'R22 group' includes three single-component fluids, R290 (propane), R1270 (propylene), and R717 (ammonia), which have very small GWPs but require

Domanski, Piotr; Cho, Hong Hyun.
"Optimized Air-to-Regerant Heat Exchanger With Low-GWP Regerants."
Paper presented at the 12th IIR Gustav Lorentzen Conference on Natural Working Fluids, Edinburgh, United Kingdom, Aug 21-Aug 24, 2016.

engineering measures to address application restrictions related to their A3, A3 and B2 safety classifications, respectively (ASHRAE, 2013). The other fluids are zeotropic mixtures designed to approximate R22 thermodynamic performance. One blend has the A1 safety designation, and the other two are mildly flammable (A2L). These blends present fewer safety-related application difficulties than R290, R1270, and R717; however, their GWPs are higher. The 'R410A group' includes two single-component fluids, R32 and R744 (carbon dioxide), which is the only non-flammable fluid. The other fluids are blends (all A2L). Generally, R744 and R717 are not considered to be direct replacement fluids. R744 has significantly higher pressure than other fluids and R717 can't be used with copper tubes and has high toxicity, but they are included here to elucidate issues of refrigerant circuitry optimization.

Table 1. Studied Alternative Low-GWP Refrigerants

(a) R22 alternative refrigerants

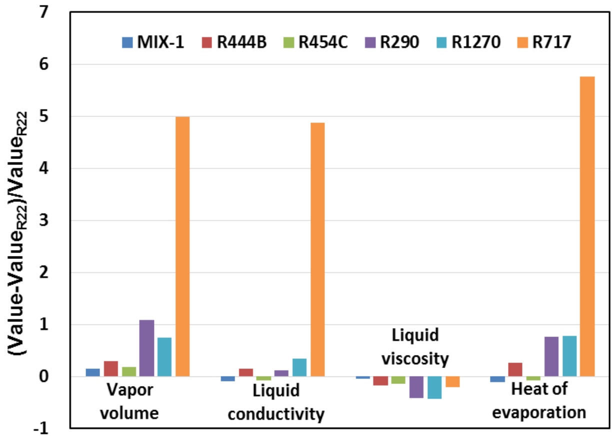
Refrigerant	Composition	Mass fraction (%)	Temperature glide[1] (K)	Safety classification[2]	GWP[3]
R22 (base)	R22	100	0	A1	1760
MIX-1[4]	R32/R125/R134a/R1234yf	13/13/31/43	4.0	A1	904
R444B	R32/R152a/R1234ze(E)	41.5/10/48.5	7.9	A2L	295
R454C	R32/R1234yf	21.5/78.5	6.1	A2L	146
R290	R290	100	0	A3	9
R1270	R1270	100	0	A3	1
R717	R717	100	0	B2	<1

(b) R410A alternative refrigerants

Refrigerant	Composition	Mass fraction (%)	Temperature glide[1] (K)	Safety classification[2]	GWP[3]
R410A(base)	R32/R125	50/50	0.1	A1	1924
MIX-2[5]	R32/R1234yf/R1234ze(E)	68/26/6	1.7	A2L	677
R32	R32	100	0	A2L	676
MIX-3[6]	R32/134a/1234ze(E)	76/6/18	2.7	A2L	593
R452B	R32/R125/R1234yf	67/7/26	1.0	A2L	572
R447A	R32/R125/R1234ze(E)	68/3.5/28.5	3.8	A2L	461
R744	R744	100	0	A1	1

[1] For isobaric evaporation at 7.2 °C dew-point temperature and inlet quality per Table 3; [2]ASHRAE (2013);
[3] Myhre at al. (2013) [4], [5], [6] Developmental names: N-20B, ARM-71A, HPR-2A, respectively

It is worthwhile to note the important parameters with regard to circuitry optimization. High liquid thermal conductivity improves the heat transfer, which reduces heat transfer irreversibilities. Low viscosity results in low pressure drop, and low drop in saturation temperature (T_{sat}) in relation to drop in pressure (P), dT_{sat}/dP, which allows for a high refrigerant mass flux to maximize the heat transfer while maintaining acceptable pressure drop. Other favorable characteristics are high heat of evaporation and high gas density. Figures 1 and 2 present properties for the studied refrigerants relative to the corresponding properties of R22 and R410A, respectively. The vapor specific volumes of R290, R1270 and R717 are much greater than that of R22, while their viscosities are lower. R717 has significantly greater liquid conductivity and heat of evaporation than R22. Other refrigerants have properties similar to those of R22. In case of 'R410A group', all alternatives except R744 have a higher specific vapor volume and liquid conductivity than R410A. R32 has the highest liquid conductivity among the alternatives. R744 has much lower vapor specific volume and liquid viscosity compared to all fluids including R410A.



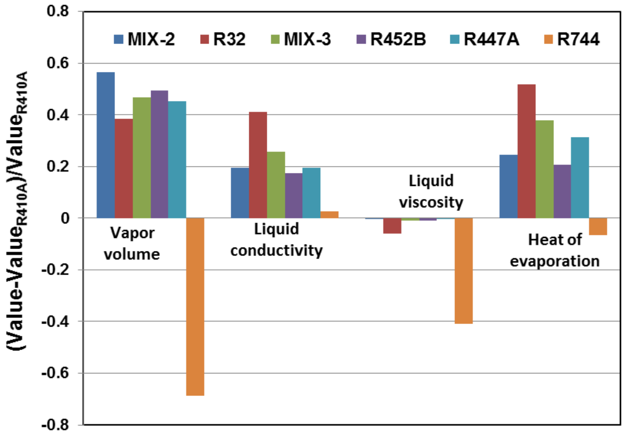


Figure 1. Vapor specific volume, liquid thermal conductivity, liquid viscosity, and heat of evaporation of R22 alternatives at 7.2 °C saturation temperature referenced to R22 properties

Figure 2. Vapor specific volume, liquid thermal conductivity, liquid viscosity, and heat of evaporation of R410A alternatives at 7.2 °C saturation temperature referenced to R410A properties

3. HEAT EXCHANGER SPECIFICATIONS

Figure 3 shows a schematic of the side view of the 60-tube heat exchanger as it is displayed by the graphical user interface of EVAP-COND, a public-domain design tool for finned-tube evaporators and condensers (Domanski et al., 2014). The circles represent the tubes, the solid lines denote return bends on the near side, and the broken lines denote return bends on the far side. The shown refrigerant circuitry is that of the original design with three inlets (tubes 1, 21, and 41) and three outlets (tubes 20, 40, and 60). This 3-circuit (3-pass) circuitry provides some level of robustness against a non-uniform inlet air distribution because each circuits extends through the whole width of the slab from the left-hand side to the right-hand side.

The shown heat exchanger was one of two identical slabs of a residential air conditioner's "A-shape" evaporator for which Yashar and Domanski (2009) measured the inlet air velocity using the particle image velocimetry method. The velocity profile (Figure 3) reflects the geometry of the "A-shape" assembly and the location of the condensate collection pan. The pan obstructs the airflow on the left-hand side of the coil, affecting heat transfer in tubes 1, 2 and 3 in the first depth row and another 6 tubes in the second and third row. We used this coil (including the inlet air velocity profile) in our study and optimized refrigerant circuitry (number of parallel circuits and tube connections) for each refrigerant. Table 2 provides the evaporator design information.

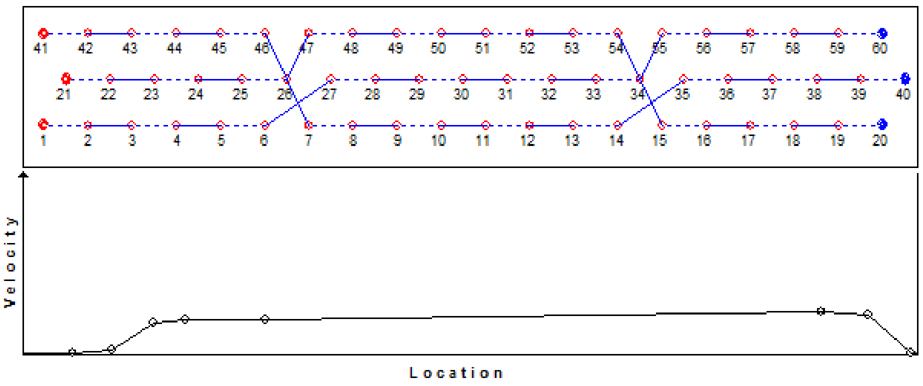


Figure 3. Side view schematic of evaporator with original tube connections and inlet air velocity profile

Table 2. Evaporator design information

Items	Unit	Value
Number of depth rows	-	3
Number of tubes per row	-	20
Tube length	mm	457
Tube pitch	mm	25.4
Tube depth row pitch	mm	19
Tube inside diameter	mm	8.7
Tube outside diameter	mm	9.5
Fin thickness	mm	0.2
Fin pitch	mm	2
Tube inner surface	-	smooth
Fin geometry	-	wavy
Tube material	-	copper
Fin material	-	aluminum
Volume flow rate of air	$m^3 s^{-1}$	0.25

Table 3. Refrigerant inlet quality

Refrigerant	Inlet quality
R22	0.176
MIX-1	0.222
R444B	0.187
R454C	0.224
R290	0.208
R1270	0.203
R717	0.108
R410A	0.220
MIX-2	0.193
R32	0.176
MIX-3	0.181
R452B	0.197
R447A	0.186
R744	0.284

4. REFRIGERANT CIRCUITRY OPTIMIZATION

4.1 Optimization Tool

We performed circuitry optimizations using the EVAP-COND package (Domanski et al., 2014). It contains first-principle-based simulation models for a finned-tube evaporator and condenser, EVAP and COND, and Intelligent System for Heat Exchanger design, ISHED. The “tube-by-tube” heat exchanger modeling scheme allows for specifying complex refrigerant circuits, modeling refrigerant distribution between these circuits, and accounting for non-uniform air distribution. Representation of refrigerant thermophysical properties is based on Lemmon et al. (2013). EVAP-COND has been validated against various experimental data sets (e.g., Payne and Domanski, 2003).

The refrigerant circuitry optimization module ISHED applies a novel methodology of *guided evolutionary computation*, which integrates methods of machine learning and evolutionary computation to assist designers in maximizing the capacity (Domanski, 2014). During the optimization run, ISHED operates on one generation (population) of circuitry architectures at a time. Each member of the population is evaluated by the heat exchanger simulator (EVAP in this study), which provides the heat exchanger’s capacity as a single numerical fitness value. The designs and their fitness values are returned to ISHED’s Control Module as an input for deriving the next generation of circuitry designs. This process continues for a number of iterations (generations) set by the user. After the specified number of iterations is performed, ISHED terminates the execution and reports on the best designs it has generated. In this work we set ISHED for 300 populations of 40 members; hence, 12 000 refrigerant circuitry architectures were evaluated during a single optimization run. More information on application of ISHED is presented in Domanski et al. (2005), Domanski and Yashar (2006), and Yashar et al. (2015), which includes a laboratory validation of the optimization process.

4.2 Operating Conditions Used for Optimization Runs

The following were evaporator operational parameters during the optimization runs:

- Inlet air condition: 26.6 °C dry-bulb temperature, 50 % relative humidity, 101.325 kPa pressure
- Volumetric airflow rate: 0.25 m^3s^{-1}
- Refrigerant quality at the evaporator inlet: as shown in Table 3
- Refrigerant saturation temperature at the evaporator exit: 7.2 °C
- Refrigerant superheat at the evaporator exit: 5.6 °C

The refrigerant inlet quality (Table 3) was established from a vapor compression cycle in which the refrigerant undergoes the isenthalpic expansion process from 42.0 °C saturation temperature with 5.0 °C subcooling to the evaporator pressure corresponding to 7.2 °C dew-point temperature and 2.0 °C saturation temperature drop between the evaporator inlet and exit. The exception was R744 for which a transcritical cycle was used with 36.0 °C gas cooler exit temperature, 80 % effective internal heat exchanger, evaporator exit dew point of 7.2 °C with a pressure drop corresponding to 1.0 °C drop in saturation temperature. It is recognized that in an actual system with optimized compressor size and condenser circuitry, the refrigerant dew-point temperature at the evaporator exit will vary between different refrigerants; however, the use of one value (7.2 °C) is adequate because small variations in the exit dew-point temperature are not expected to change the outcome of the refrigerant circuitry optimization process.

5. OPTIMIZATION RESULTS

5.1 Performance with Refrigerant Circuitries Optimized for R22 and R410A

The symmetric layout of the original circuitry with three circuits extending through the whole width of the coil provides some level of robustness for operation with non-uniform air distribution. Nevertheless, as a preliminary step, we explored the benefit of optimization that included the measured non-uniform air distribution (Figure 3). We optimized the circuitries for R22 and R410A and then applied these optimized circuitries to other fluids. This task yielded mixed results. Figures 4 and 5 present changes in capacity (difference between capacity with the optimized circuitry for R22 or R410A, $Q_{\mathrm{OPT,R22}}$ or $Q_{\mathrm{OPT,R410A}}$, and the capacity of the refrigerant attained with the original circuitry Q_{ORG}, referenced to Q_{ORG}). The capacity of R22 improved by 1.9 %. Among other fluids from the ‘R22 group’, R290, R1270, and R717 (single-component fluids) benefited between from 2 to 3.5 times as much as R22; however, performance of zeotropic blends deteriorated. For the higher-pressure ‘R410A group’, capacities of all refrigerants improved by over 6 %. The lowest gain is shown for R447A, which has the highest two-phase temperature glide in this group. This task emphasized the challenge and need for optimizing refrigerant circuitries for zeotropic mixtures.

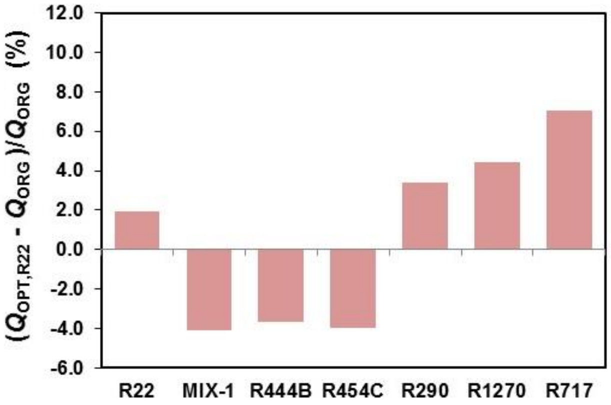


Figure 4. Capacity change for R22 and R22 alternatives with refrigerant circuitry optimized for R22 referenced to the capacity obtained by this refrigerant with the original circuitry

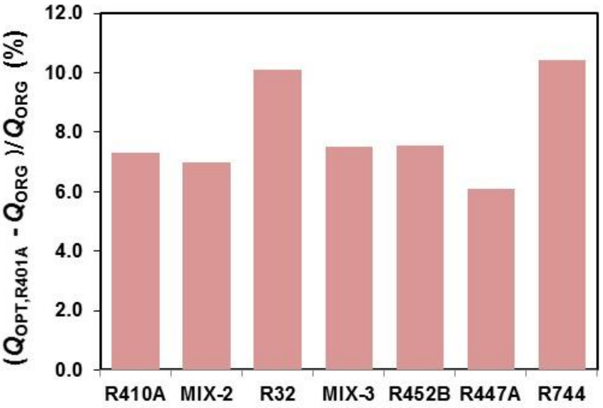


Figure 5. Capacity change for R410A and R410A alternatives with refrigerant circuitry optimized for R410A referenced to the capacity obtained by this refrigerant with the original circuitry

5.2 Performance with Refrigerant Circuitries Optimized for Each Refrigerants

With the aid of ISHED, we developed optimized circuitries for each refrigerant. As expected, each refrigerant benefited from the optimized circuitry (Figures 6 and 7). On average, the ‘R410A group’ (high-pressure refrigerants) benefited more from the optimization than the ‘R22 group’, and R22 benefited the least. These results may be related to the fact that the studied evaporator was originally designed as a component of an R22 residential air conditioner and was already optimized for R22 using traditional optimization methods. The R22 improvement may be related to ability of the ISHED-optimized design to accommodate the minimal airflow for tubes 1, 2, 3 in the first depth row and their counterparts in the second and third depth row. Examining individual fluids, capacity increases of R744 and R32 were the largest, above 12 %. In the lower-pressure ‘R22 group’ the largest capacity gain is shown for ammonia, above 10 %. All these fluids have outstanding thermodynamic and transport properties.

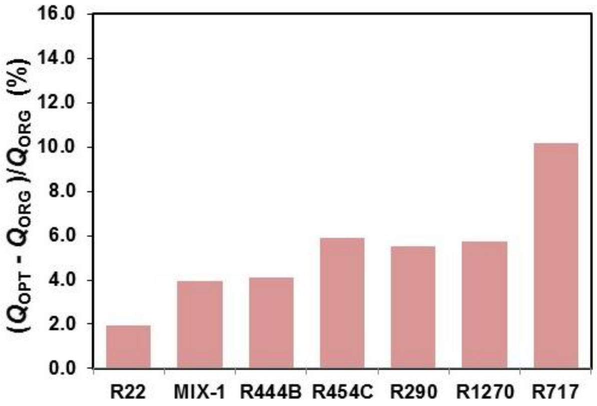


Figure 6. Capacity improvement for R22 and R22 alternatives with refrigerant circuitry optimized for each individual refrigerant referenced to the capacity obtained by this fluid with the original circuitry

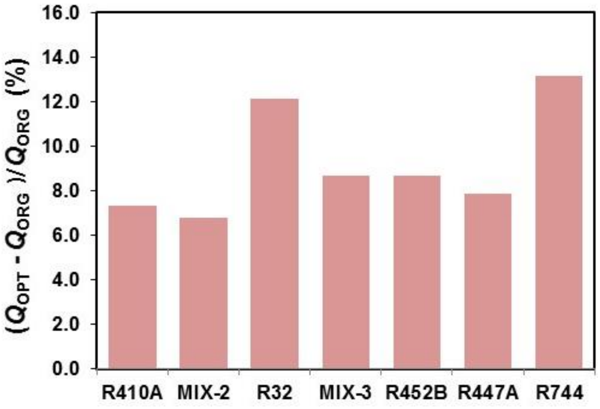


Figure 7. Capacity improvement for R410A and R410A alternatives with refrigerant circuitry optimized for each fluid referenced to the capacity obtained by this fluid with original circuitry

Table 4 presents the number of inlet and outlet tubes in the circuitries optimized for each refrigerant. For the ‘R410A group’, five out of seven refrigerants have one inlet tube and two outlet tubes. The highest-pressure refrigerant in the group, R744, has just one refrigerant pass, and R447A has two inlets and three outlets. The ‘R22 group’ (the lower-pressure group) has only R1270 in the one-inlet/two-outlets category, three refrigerants with two inlets and two outlets, R454C with two inlets and three outlets, and MIX-1 and R717 with the least restrictive circuitry using two inlets and four outlets. In general, circuitries for lower-pressure refrigerants have more parallel passes and are less restrictive to avoid excessive pressure drop and the associated drop in saturation temperature. Higher-pressure refrigerants exhibit a smaller drop of saturation temperature for a given pressure drop; this allows them to use more restrictive circuitries, which results in higher refrigerant mass fluxes and enhanced heat transfer at acceptable penalty of the saturation temperature drop. In an initially perplexing case of the least restrictive circuitry assigned for R717, reducing R717 heat transfer resistance through increasing mass flux is not beneficial because R717 heat transfer resistance is small due the outstanding thermal conductivity (particularly that of liquid), which makes the dominant share of heat transfer resistance on the air side. In this case, the penalty of the saturation temperature drop of R717 becomes the more influential factor than heat transfer improvement.

Table 4. Number of inlet and outlet tubes in ISHED-optimized circuitries[(a)]

		Number of outlet tubes			
		1	2	3	4
Number of inlet tubes	1	**R744**	**R410A, MIX-2, R32, R452B, MIX-3,** R1270		
	2		R22, R444B, R290	**R447A,** R454C	MIX-1, R717

[(a)] Bold font denotes the ‘R410A group’; normal font denotes the ‘R22 group’

We should note that the level of changes in evaporator capacity obtained through optimization at the same dew-point temperature at the evaporator exit will not be achieved in the actual system because the system rebalances itself at a different evaporator dew-point temperature once an evaporator of different capacity is installed. But, the results presented in Figures 6 and 7 let us estimate the system capacity and COP changes by using a simplified rating procedure for so called 'mixed systems' (Domanski, 1989). This simplified procedure applies an exponent of 0.35 and 0.21 to the evaporator capacity ratio (new evaporator over old evaporator) to estimate a change in system capacity and COP. Following this procedure, a 10 % improvement in capacity results in 3.4 % ($1.1^{0.35}$) and 2.0 % ($1.1^{0.21}$) improvement in system capacity and COP, respectively, over the values in the system with the original evaporator. For the data presented in Figure 6 and 7, the system measurements from 'drop in' tests could be better by 1 % to 4 % for the capacity and 1 % to 2.5 % for the COP. We need to emphasize the speculative nature of this assessment since the possible improvement depends on the design of the original evaporator and thermophysical characteristics of a new fluid.

Table 5 shows selected absolute performance information for circuitries optimized for each refrigerant. Overall, the high-pressure 'R410A group' shows higher capacities than the 'R22 group'. Within each group, R444B and R447A (zeotropic blends with the highest temperature glide) have the highest capacities because our simulations at the same dew-point temperature at the evaporator exit (7.2 °C) gave them the advantage of an increased mean effective temperature between the refrigerant and the air. For some zeotropes their two-phase glide was mitigated by the pressure drop. The outstanding performance of R717 was achieved on the strength of its thermophysical properties. The column with volumetric flow rate provides an indication on the compressor size required for individual refrigerants. Actual performance in a system will be also affected by the performance of the condenser and the overall system balance.

Table 5. Performance information for circuitries optimized for each refrigerant

(a) R22 alternative refrigerants

Refrigerant	Capacity (kW)	Mass flow rate ($kg \cdot h^{-1}$)	Pressure drop (kPa)	$T_{dew\text{-}point}$ drop due to pressure drop (K)	Two-phase temperature change$^{(1)}$ (K)	Volumetric flow rate$^{(2)}$ (m^3s^{-1})
R22	5.22	114.0	56.0	2.8	-2.8	$1.23 \cdot 10^{-3}$
MIX-1	6.07	149.6	36.4	2.1	1.9	$1.68 \cdot 10^{-3}$
R444B	6.96	124.2	33.7	1.9	6.0	$1.80 \cdot 10^{-3}$
R454C	6.56	159.3	40.7	2.3	3.8	$1.76 \cdot 10^{-3}$
R290	5.49	69.1	40.7	2.3	-2.3	$1.55 \cdot 10^{-3}$
R1270	5.67	68.7	43.8	2.1	-2.1	$1.30 \cdot 10^{-3}$
R717	6.32	20.3	17.3	0.8	-0.8	$1.30 \cdot 10^{-3}$

(b) R410A alternative refrigerants

Refrigerant	Capacity (kW)	Mass flow rate ($kg \cdot h^{-1}$)	Pressure drop (kPa)	$T_{dew\text{-}point}$ drop due to pressure drop (K)	Two-phase temperature change$^{(1)}$ (K)	Volumetric flow rate$^{(2)}$ (m^3s^{-1})
R410A	5.82	124.9	60.3	2.0	-1.9	$9.38 \cdot 10^{-4}$
MIX-2	6.12	106.6	55.6	2.0	-0.3	$1.06 \cdot 10^{-3}$
R32	6.00	85.1	35.4	1.1	-1.1	$8.83 \cdot 10^{-4}$
MIX-3	6.51	103.6	55.7	2.1	0.6	$1.15 \cdot 10^{-3}$
R452B	5.98	106.9	50.5	1.8	-0.8	$1.00 \cdot 10^{-3}$
R447A	6.69	112.4	67.1	2.6	1.2	$1.10 \cdot 10^{-3}$
R744	6.29	143.7	103.9	1.0	-1.0	$2.98 \cdot 10^{-3}$

(1) Isobaric two-phase temperature glide from inlet to outlet minus the drop of dew-point temperature, $T_{dew\text{-}point}$, due to pressure drop; (2) At the evaporator outlet

6. CONCLUDING REMARKS

We investigated the effect of an optimized refrigerant circuitry on the evaporator capacity for twelve R22 and R410A low-GWP alternative fluids. All fluids benefited from the optimization process carried out specifically for individual refrigerants. High-pressure refrigerants benefited most with R744 achieving a capacity increase of over 13 %, and all other achieving over 6 % improvement. Among lower-pressure refrigerants, capacity gains for R290, R1270, and R454C were over 5.5 %, and the capacity improvement for R717 was over 10 %. Smaller capacity improvements will be achieved in a complete system because of rebalancing of the system upon installation of a more effective evaporator. If optimized refrigerant circuitries were implemented in alternative refrigerant tests in existing equipment (hypothetical for ammonia and R744), these as-installed capacity improvements are estimated to be within 1 % to 4 %, and will be associated with 1 % to 2.5 % increases in the system COP over "drop-in" test results for the studied cases. Additional performance gains can be achieved through optimization of other components. The optimization results demonstrated that zeotropic blends with a significant temperature glide are particularly sensitive to the layout of refrigerant circuitry and may suffer significant performance degradation due to an improper circuitry design.

REFERENCES

Abdelaziz, O., Shrestha, S., Munk, J., Linkous, R., Goetzler, W., Guernsey, M., Kassuga, T., 2015. Alternative Refrigerant Evaluation for High-Ambient-Temperature Environments: R-22 and R-410A Alternatives for Mini-Split Air Conditioners, ORLL/TM-2015/536.

ASHRAE, 2013. ANSI/ASHRAE Standard 34-2013 Designation and Safety Classification of Refrigerants. ASHRAE, Atlanta.

Domanski, P.A., Yashar, D.A, Wojtusiak, J., 2014. EVAP-COND, Version 4.0: Simulation Models for Finned-Tube Heat Exchangers with Circuitry Optimization. National Institute of Standards and Technology, Gaithersburg, MD., http://www.nist.gov/el/building_environment/evapcond_software.cfm

Domanski, P. A., Yashar, D. A., 2007. Optimization of Finned-Tube Condensers Using an Intelligent System. Int. J. Refrig. 30 (3), 482-488.

Domanski, P.A., Yashar, D., 2006. Comparable Performance Evaluation of HC and HFC Refrigerants in an Optimized System, 7th IIR Gustav Lorentzen Conference on Natural Working Fluids, Trondheim, Norway.

Domanski, P.A., Yashar, D., Kim, M., 2005. Performance of a finned-tube evaporator optimized for different refrigerants and its effect on system efficiency, *Int. J. Refrig*., 28 (6): 820-827.

Domanski, P.A., Yashar, D., Kaufman, KA., Michalski R.S., 2004. Optimized design of finned-tube evaporators using learnable evolution methods. *Int. J. HVAC&R Research*, 10(2): 201-212.

Domanski, P.A., 1989. Rating Procedure for Mixed Air Source Unitary Air Conditioners and Heat Pumps Operating in the Cooling Mode - Revision 1, NISTIR 89-4071, National Institute of Standards and Technology, Gaithersburg, MD

EU, 2014. Regulation No 517/2014 of the European Parliament and of the Council of 16 April 2014 on fluorinated greenhouse gases and repealing Regulation (EC) No 842/2006 (2014).

Lemmon, E.W., Huber, M.L., McLinden, M.O., 2013. NIST Standard Reference Database 23, NIST Reference Fluid Thermodynamic and Transport Properties—REFPROP, Version 9.1. Standard Reference Data Program, National Institute of Standards and Technology, Gaithersburg, MD.

Myhre, G., D. Shindell, F.-M. Bréon, W. Collins, J. Fuglestvedt, J. Huang, D. Koch, J.-F. Lamarque, D. Lee, B. Mendoza, T. Nakajima, A. Robock, G. Stephens, T. Takemura H. Zhang, 2013. Anthropogenic and Natural Radiative Forcing, Section 8 in: *Climate Change 2013: The Physical Science Basis, Fifth Assessment Report of the Intergovernmental Panel on Climate Change*. Cambridge, UK, Cambridge University Press.

Payne W. V., Domanski, P.A., 2003. Potential Benefits of Smart Refrigerant Distributors, report to Air-Conditioning and Refrigeration Technology Institute, report ARTI-21CR/605-200-50-01.

Yashar, D.A., Domanski, P.A., 2009. Particle Image Velocimetry Measurements and CFD-Based Predictions of Air Distribution at Evaporator Inlet and Outlet, NIST TN 1651, National Institute of Standards and Technology, Gaithersburg, MD.

Yashar, D.A., Domanski, P.A., Lee, S., 2010. Evaporator Optimization for Non-Uniform Air Distribution. Proceedings of Conference of Sustainable Refrigeration and Heat Pump Technology, Stockholm, Sweden.

Yashar, D.A., Lee, S., Domanski, P.A., 2015. Rooftop Air-Conditioning Unit Performance Improvement Using Refrigerant Circuitry Optimization, Applied Thermal Engineering, 83:81-87.

The NIST IAD Data Science Evaluation Series: Part of the NIST Information Access Division Data Science Research Program

Bonnie J. Dorr*, Craig S. Greenberg*, Peter Fontana*, Mark Przybocki*,
Marion Le Bras*†, Cathryn Ploehn*, Oleg Aulov*, and Wo Chang*
*National Institute of Standards and Technology
†Guest Researcher
{bonnie.dorr,craig.greenberg,peter.fontana,mark.przybocki,
marion.lebras,cathryn.ploehn,oleg.aulov,wchang}@nist.gov

***Abstract*—The Information Access Division (IAD) of the National Institute of Standards and Technology (NIST) launched a new Data Science Research Program (DSRP) in the fall of 2015. This research program focuses on evaluation-driven research and will establish a new Data Science Evaluation series to facilitate research collaboration, to leverage shared technology and infrastructure, and to further build and strengthen the data science community. The evaluation series will consist of a pre-pilot to be launched in the fall of 2015, a pilot evaluation to be launched in 2016, and a full-scale multiple-track evaluation in 2017. In addition to these evaluations, this new research program aims to address several infrastructure challenges and to encourage easier group collaboration.**

I. Summary

The Information Access Division (IAD) of the National Institute of Standards and Technology (NIST) is launching a new Data Science Research Program (DSRP) in the Fall of 2015. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. Through this research program, NIST aims to provide a framework for the research community to examine a range of different algorithms and methodologies in data science (DS) and to address current challenges and breakthroughs in data science. The DSRP focuses on building domain-independent solutions, i.e., those that can solve a variety of data science challenges across different data domains. The components of the DSRP are summarized in Figure 1. These four key components are:

- **Evaluation and Metrology**: Design and conduct a new international *Data Science Evaluation (DSE)* series.
- **Standards:** Leverage prior work to develop standards for data science.
- **Compute Infrastructure:** Develop an Evaluation Management System (EMS) to support compute and infrastructure needs including test and evaluation (T&E) of different compute paradigms
- **Community Outreach:** Build a community of interest within which data scientists can more effectively collaborate through coordination of their efforts on similar classes of problems.

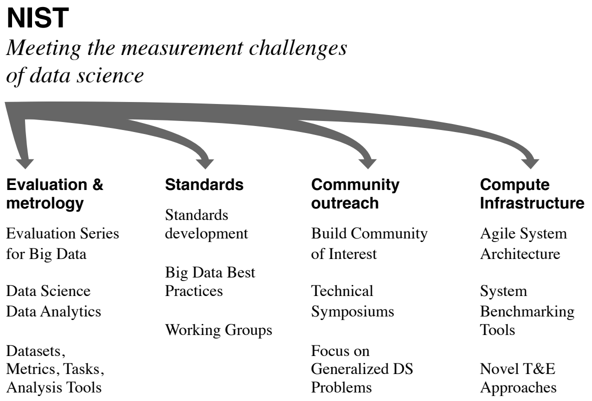

NIST
Meeting the measurement challenges of data science
Evaluation & metrology
Evaluation Series for Big Data
Data Science Data Analytics
Datasets, Metrics, Tasks, Analysis Tools
Standards
Standards development
Big Data Best Practices
Working Groups
Community outreach
Build Community of Interest
Technical Symposiums
Focus on Generalized DS Problems
Compute Infrastructure
Agile System Architecture
System Benchmarking Tools
Novel T&E Approaches

Fig. 1. A summary of the NIST Data Science Research Program. Figure is from [1].

Dorr et al. [1] present more information on this research program, including background and additional citations.

One critical component of the DSRP is the DSE. The DSE series will consist of regularly scheduled evaluations, expected to recur annually. Each evaluation in the series will consist of several tracks, where a track is made up of challenge problems set in a given domain. In addition to evaluator-hosted tracks, the DSE series will include community-championed tracks. Track proposals will be solicited from the community, and each track included in the evaluation will be planned, organized, and implemented by a "track champion" from within the community.

The DSE series will be developed in three stages: a pre-pilot evaluation that will consist of a single track with a traffic prediction use case, a pilot evaluation that will extend the pre-pilot evaluation-track and will be open to all who wish to participate, and an inaugural evaluation that will consist of multiple community-led evaluation tracks in different domains and use cases. This sequence will enable immediate deployment of a new infrastructure for addressing data science research challenges. This infrastructure will be leveraged for

Dorr, Bonnie; Greenberg, Craig; Fontana, Peter; Przybocki, Mark; Le Bras, Marion; Ploehn, Cathryn; Aulov, Oleg; Chang, Wo.
"The NIST IAD Data Science Evaluation Series: Part of the NIST Information Access Division Data Science Research Program."
Paper presented at the 2015 IEEE International Conference on Big Data, Santa Clara, CA, Oct 29-Nov 1, 2015.

rapid development and evolution of the DSE series and will effectively enable generalizations to multiple domains and tracks.

II. Evaluation-Driven Research

The core of the DSE is to leverage the framework of evaluation-driven research and to apply it to the area of data science.

The process for evaluation-driven research can be divided into four steps:

1) *Planning.*, Planning includes defining the task and research objectives for the evaluation. It should be noted that only so many objectives can be pursued at once; it is therefore essential to choose objectives that will substantially improve the technology while being challenging but reachable in the near term. Receiving community input during this step is critical.
2) *Data and experiment design.*, The experiment design involves developing datasets and associated tasks for experimentation. For example, in machine learning, data are typically partitioned into training, development, and evaluation datasets. An example of a possible experiment is to contrast performance using different training datasets. Rigorously designing experiments and datasets is significantly easier when the data to be used was created for the evaluation (as opposed to being repurposed), though data collection design and implementation has its own challenges (for example see [2]).
3) *Performance assessment.* After the experiment is designed, the performances of the systems are evaluated. In this stage, systems are trained on the training data and run on the test data. In some evaluations, the data is sent to researchers, who run their systems locally and then submit their systems' outputs. In other evaluations, the systems themselves are submitted and then are run by the evaluator. The latter approach is more involved and requires an agreed upon API and ability for every system to run on a prescribed computational infrastructure, though is better suited for evaluations using very large or sensitive datasets. Once system outputs are generated, the experimental results are analyzed.
4) *Workshop.* After the performance assessment, a workshop is held. At this workshop, the research community gathers to openly discuss research in the context of a shared evaluation, evaluation outcomes, including which approaches were attempted and the degree to which they were successful, as well as other lessons learned. A crucial portion of the workshop is a discussion of future challenges and objectives, which feeds into the planning of the next evaluation. Beyond the workshop, evaluation results are published more broadly.

These four steps naturally form a cycle, wherein the planning for an evaluation takes place, in part, at the workshop of the previous evaluation. See Figure 2 for an illustration.

Progress is driven in evaluation-driven research by repeating the evaluation cycle and, as technology improves, increasing the challenge of the research objectives, which are then addressed in subsequent evaluations. After the technology reaches a point appropriate for a given application, engineering for speed and other considerations takes place and the technology is deployed for the application. The evaluation cycle continues, driving more technological progress to enable transfer to more demanding applications. It is worth noting that the evaluator's roles in data-centric technology transfer are typically focused on the relatively early and late stages of the process, i.e., core technology research and standards, respectively.

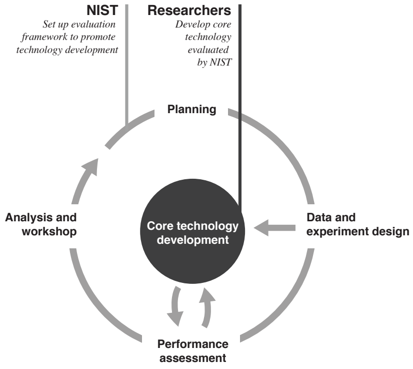

NIST
Set up evaluation framework to promote technology development
Researchers
Develop core technology evaluated by NIST
Planning
Analysis and workshop
Core technology development
Data and experiment design
Performance assessment

Fig. 2. Overview of the evaluation-driven research cycle.

III. Evaluation Timeline

The evaluation pre-pilot will take place in the fall of 2015. In 2016, an evaluation pilot will be conducted and track proposals will be accepted for a 2017 full-scale data science evaluation. A summary of the DSE is in Figure 3.

Details about the pre-pilot, which is currently underway, are provided in Figures 4, 5, and 6. The data and tasks for the pre-pilot are set in the traffic domain—a domain chosen due to its relevance to everyday life of the general public and due to the accessibility and availability of large amounts of public data associated with this domain. It is important to note that, although the pre-pilot focuses on the traffic domain, the objective is for the developed measurement methods and techniques to apply to additional use cases, regardless of the domain and data characteristics.

Lessons learned from the pre-pilot will be leveraged for development of a larger-scale pilot evaluation, which will still be in the traffic prediction domain. After the pilot, a multi-track full-scale evaluation will be conducted—the first full evaluation in the series.

IV. Conclusion

In summary, the goals of the Data Science Research Program and the Data Science Evaluation Series are:

- to further build and strengthen the data science community,
- to address infrastructure challenges, and
- to provide standards to facilitate group collaboration.

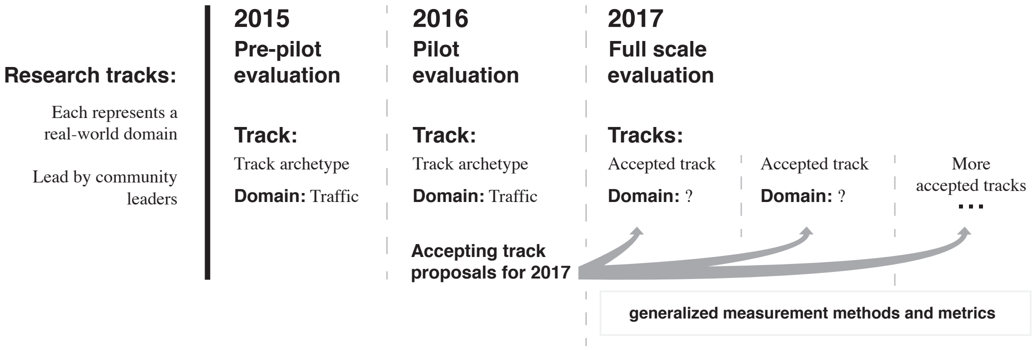
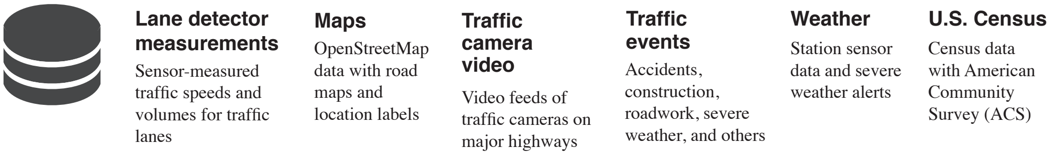
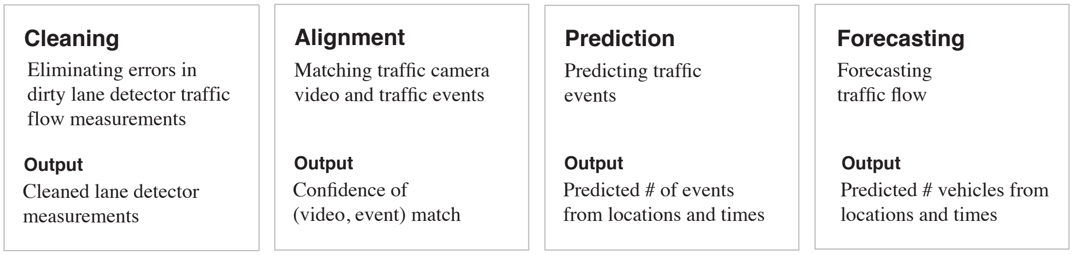


Fig. 3. Overview of the data science evaluation series.



Lane detector measurements
Sensor-measured traffic speeds and volumes for traffic lanes
Maps
OpenStreetMap data with road maps and location labels
Traffic camera video
Video feeds of traffic cameras on major highways
Traffic events
Accidents, construction, roadwork, severe weather, and others
Weather
Station sensor data and severe weather alerts
U.S. Census
Census data with American Community Survey (ACS)

Fig. 4. Summary of the data available for use in the pre-pilot.



Cleaning
Eliminating errors in dirty lane detector traffic flow measurements
Output
Cleaned lane detector measurements
Alignment
Matching traffic camera video and traffic events
Output
Confidence of (video, event) match
Prediction
Predicting traffic events
Output
Predicted # of events from locations and times
Forecasting
Forecasting traffic flow
Output
Predicted # vehicles from locations and times

Fig. 5. Summary description of the four tasks in the pre-pilot.

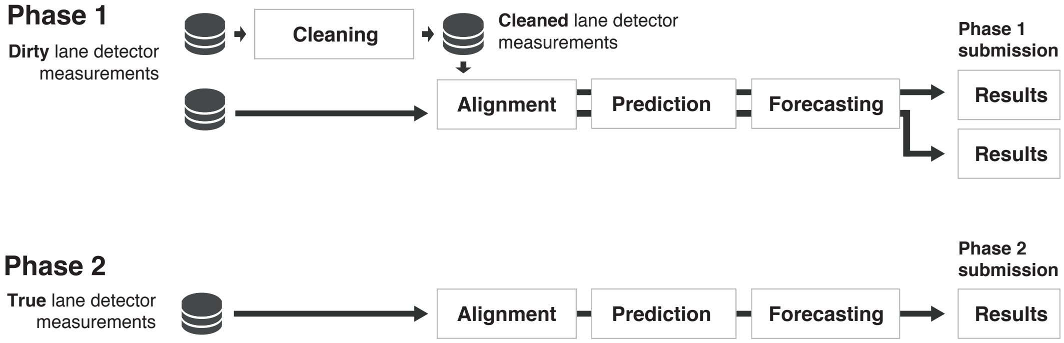


Fig. 6. Summary of the evaluation flow of the Pre-Pilot evaluation. In phase one, participants submit two sets of results for the alignment, prediction, and forecasting tasks: one submission using the original dirty traffic lane detector data, and a second using the cleaned traffic detector data, which is the output of the cleaning task.

References

[1] B. J. Dorr, C. S. Greenberg, P. Fontana, M. Przybocki, M. Le Bras, C. Ploehn, O. Aulov, M. Michel, E. Golden, and W. Chang, "The NIST data science initiative," in *To appear in the proceedings of the IEEE International Conference on Data Science and Advanced Analytics (DSAA)*. IEEE, October 2015.

[2] K. Gallagher, A. Stanley, D. Shearer, and L. V. Klerman, "Challenges in data collection, analysis, and distribution of information in community coalition demonstration projects," *Journal of Adolescent Health*, vol. 37, no. 3, Supplement, pp. S53–S60, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1054139X05002508

The NIST IAD Data Science Research Program

Bonnie J. Dorr*, Craig S. Greenberg*, Peter Fontana*, Mark Przybocki*,
Marion Le Bras*‡, Cathryn Ploehn*, Oleg Aulov†, Martial Michel*, E. Jim Golden*, and Wo Chang*
*National Institute of Standards and Technology
†University of Maryland, Baltimore County
‡Guest Researcher
{bonnie.dorr,craig.greenberg,peter.fontana,mark.przybocki,
marion.lebras,cathryn.ploehn,oleg.aulov,martial.michel,edmond.golden,wchang}@nist.gov

***Abstract*—We examine foundational issues in data science including current challenges, basic research questions, and expected advances, as the basis for a new Data Science Research Program and evaluation series, introduced by the Information Access Division (IAD) of the National Institute of Standards and Technology (NIST) in the fall of 2015. The evaluations will facilitate research efforts, collaboration, leverage shared infrastructure, and effectively address cross-cutting challenges faced by diverse data science communities. The evaluations will have multiple research tracks championed by members of the data science community, and will enable rigorous comparison of approaches through common tasks, datasets, metrics, and shared research challenges. The tracks will measure several different data science technologies in a wide range of fields, starting with a pre-pilot. In addition to developing data science evaluation methods and metrics, it will address computing infrastructure, standards for an interoperability framework, and domain-specific examples.**

I. Introduction

Since its emergence as a uniquely identifiable field, *data science* has been of growing importance, attested to by a proliferation of government initiatives[1], research conferences[2], and academic data science initiatives and institutes[3]. As in any rapidly emerging field, there is a pressing need to explore the foundational issues underpinning data science. Indeed, the “Trends and Controversies” presented at the Data Science and Advanced Analysis conference in 2014 [2] raised a range of data science challenges, research questions, and expected advances.

A new Data Science Research Program (DSRP) introduced by the Information Access Division (IAD) of the National Institute of Standards and Technology (NIST), beginning in the fall of 2015, addresses many of the issues raised. The DSRP aims to facilitate and accelerate research progress in the field. Here, *data science* is viewed as the application of techniques for analysis and extraction of knowledge from potentially massive data. This includes notions of *big data* technical challenges in distributed and parallel processing, processing speed, and storage architectures for high *Volume* and *Velocity*, as well as the unique challenges for data visualization. The DSRP also encompasses considerations and insights that might be central even with datasets that are smaller, such as data diversity (*Variety*) and data uncertainty (*Veracity*).

The above discussion brings to light the inherent breadth of data science (DS)—spanning systems (including databases), programming languages, machine learning, statistics, and visualization, and a myriad of other disciplines, including (broadly) the natural sciences, applied sciences, and humanities. This necessary but overwhelming breadth makes clear the need to foster collaboration, provide the opportunity to coordinate research efforts, and leverage shared infrastructure across diverse communities, which are all needed in order to accelerate progress and to effectively address the present cross-cutting challenges. Several of these challenges are described in this paper.

In order to address this need, the DSRP will be developed initially[4] by means of the following four key elements:

- **Evaluation and Metrology**: Design and conduct a new international *Data Science Evaluation (DSE)* series (Section II).
- **Standards:** Leverage prior work to develop standards for data science (Section III).
- **Compute Infrastructure:** Develop an Evaluation Management System (EMS) to support compute and infrastructure needs (Section IV).
- **Community Outreach:** Build a community of interest within which data scientists can more effectively collaborate through coordination of their efforts on similar classes of problems (Section V).

A further breakdown of the elements making up this research program are outlined in Figure 1.

U.S. Government work not protected by U.S. copyright

[1] Examples include: DARPA’s announcement of the XDATA Program, NSF announcement of new Big Data solicitation of $10 million in March of 2012, NIH announced recruitment of an associate director for Data Science in 2013. Additionally, the White House appointed the first U.S. Chief Data Scientist in Feb 2015 [1]

[2] Such as: ACM’s International Conference on Knowledge Discovery and Data Mining; International Conference on Big Data Analytics; IEEE’s International Conference on Cloud and Big Data Computing, and International Conference on Data Science and Advanced Analytics

[3] For instance: Columbia University’s announcement to create Data Sciences Institute, UC Berkeley announces first online Master of Information and Data Science degree, UMass Amherst establishes Center for Data Science, University of Michigan establishes a new data science major.

[4] As a multi-year research program, the make-up of the DSRP is expected to change and grow over time as the field and technology matures.

Dorr, Bonnie; Fontana, Peter; Greenberg, Craig; Przybocki, Mark; Le Bras, Marion;
Ploehn, Cathryn; Aulov, Oleg; Michel, Martial; Golden III, Edd; Chang, Wo.
“The NIST IAD Data Science Research Program.”
Paper presented at the 2015 IEEE International Conference on Data Science and Advanced Analytics, Paris, France, Oct 19-Oct 21, 2015.

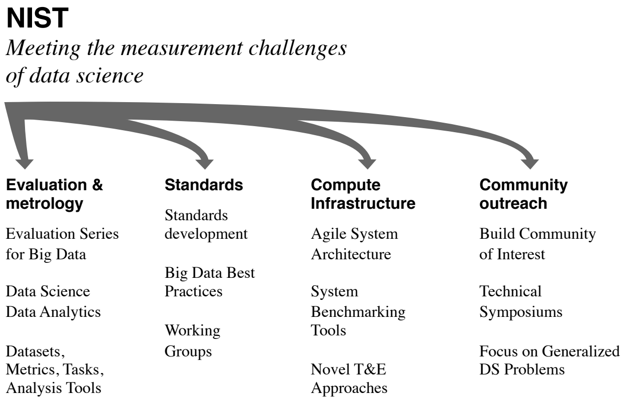

NIST
Meeting the measurement challenges of data science
Evaluation & metrology
Evaluation Series for Big Data
Data Science Data Analytics
Datasets, Metrics, Tasks, Analysis Tools
Standards
Standards development
Big Data Best Practices
Working Groups
Compute Infrastructure
Agile System Architecture
System Benchmarking Tools
Novel T&E Approaches
Community outreach
Build Community of Interest
Technical Symposiums
Focus on Generalized DS Problems

Fig. 1. NIST's role in addressing data science challenges.

This paper contains no new and novel algorithms, experiments, or results. Nor does it prescribe specific methodologies or solutions. Instead, it discusses a range of foundational data-science challenges as well as the advances necessary to drive data science forward. The contributions of this work are (1) the clear identification and examination of challenges and advances relevant to the data science community; (2) a presentation of enabling infrastructure to support research progress in data science, including the fostering of collaboration across different research communities.

The remainder of this paper describes some of the potential future breakthroughs in data science (Section VI); presents a summary of next generation of data science challenges (Section VII); categorizes different types of data science problems into explicit classes (Section VIII); discusses aspects of data science measurement (Section IX); and the final section delivers concluding remarks regarding IAD's role in the discipline of data science.

II. Evaluation and Metrology for Data Science

NIST has been conducting evaluations of data-centric technologies since the late 1980's. These evaluations cover a wide range of technologies including: automatic speech transcription, information retrieval, machine translation, speaker and language recognition, automatic fingerprint matching, image recognition, event detection from text, video, and multimedia, and automatic knowledge base construction, among many others.

Despite the stark differences among the technologies listed above, each evaluation has enabled rigorous research by sharing the following fundamental elements: (1) the use of common tasks, datasets, and metrics; (2) the presence of specific research challenges meant to drive the technology forward; (3) an infrastructure for developing effective measurement techniques and measuring the state-of-the-art; and (4) a venue for encouraging innovative algorithmic approaches. Several NIST evaluations have enjoyed substantial popularity and provided the necessary infrastructure to accelerate research progress in the corresponding core technologies.

To address several unique challenges in the burgeoning field of data science, NIST has launched the Data Science Evaluation series (DSE), to occur annually starting in the fall of 2015. These challenges stem from some combination of data characteristics (e.g., very large datasets, multi-modal datasets, data from multiple sources with varying degrees of reliability and noise) and task requirements (e.g., building of multi-component systems, enabling effective human-in-the-loop interaction, and visualization of large and complex data).

These in turn lead to various evaluation design and implementation challenges: (1) logistical aspects of conducting very large-scale evaluations, including dataset creation and distribution, and of conducting multi-component evaluations requiring coordination and timing of individual component evaluation; (2) evaluation design challenges associated with the use of "found" data rather than data collected in a controlled manner, which increases the difficulty of conducting rigorous experiments; (3) measurement challenges arising from a lack of hand-annotated data or ground truth more generally; (4) measurement and calibration of data and system uncertainty; and (5) measurement of the effectiveness of visualization. In addition, many existing research communities are formed around individual tasks, domains, or modalities—thus a multi-modal, multi-task evaluation will require the integration of multiple disparate communities.

While previous NIST evaluations have dealt with some of the challenges above, many remain unsolved. Successful data science evaluations will require addressing many of these challenges simultaneously, and in new combinations. To that end, each year of the DSE will consist of multiple research tracks—organized by domain—encouraging tasks spanning multiple tracks. In addition to one or more NIST-led tracks, community-led tracks will be included in the DSE.

As a first step, in fall of 2015, NIST will host a small scale pre-pilot evaluation in the highway traffic domain, meant to serve as a track archetype,[5] and to surface any unexpected evaluation challenges. It will consist of heterogeneous data from traffic and weather sensors and will feature data cleaning, dataset alignment, and predictive analytics tasks. In 2016, NIST will follow up with an open pilot evaluation in the same domain and will begin accepting track proposals for a 2017 full-scale data science evaluation.

III. Standards for Data Science

The design of the new DSRP leverages prior work at NIST on standards for data science, starting with those developed for big data [3]. For example, the NIST Big Data Public Working Group (NBD-PWG) developed a consensus-based, extensible interoperability framework that is vendor-neutral, technology-independent, and infrastructure-independent [4]. This framework allows data scientists to process and derive knowledge through the use of a standard interface between swappable architectural components. The following elements

[5] It's worth emphasizing the fact that this track is meant to serve as an exemplar of a data science evaluation track, not to solve any particular problem in the traffic domain.

have been formalized by the NBD-PWG—as components of a Reference Architecture ecosystem—and are expected to apply to problems in data science more generally:

- **System Orchestrator (or data scientist)**: Provides a high-level design of the dataflow between analytics tools and given datasets, computing system requirements, and monitoring system resource and performance.
- **Data Provider**: Provides an abstraction of various types of data sources (such as raw data or data previously transformed by another system) and makes them available through different functional interfaces. This includes the transfer of analytics codes to data sources for effective analytic processing.
- **Application Provider**: Provides analytics processing throughout the data lifecycle—acquisition, curation, analysis, visualization, and access—to meet requirements established by the System Orchestrator.
- **Framework Provider**: Provides one or more instances of a computing environment to support general data science tools, distributed file systems, and computing infrastructure—to meet requirements established by the Application Provider.
- **Data Consumer**: Provides an interface to receive the value output from this Reference Architecture ecosystem.
- **Security and Privacy Fabric**: Provides the security and privacy interaction to the rest of the Reference Architecture components (via the System Orchestrator) to ensure protection of data and their content.
- **Management Fabric**: Provides management interaction to other Reference Architecture components (via the System Orchestrator) with versatile system and software provisioning, resource and performance monitoring, while maintaining data quality and secure accessibility.

Recently, the NBD-PWG released working drafts of the interoperability framework for public comment [5]. These include basic definitions (concepts and vocabulary), taxonomies, use cases, reference architecture, a standards roadmap, and other elements associated with big data that are expected to apply to the space of problems in data science more generally. This framework will be released in three stages, each corresponding to a major activity relevant to the more general data science endeavor: (1) Identification of a high-level reference architecture with the following critical components: technology, infrastructure, and vendor-agnostic capability; (2) Definition of general interfaces between the reference architecture components; (3) Validation of the reference architecture by building applications through the general interfaces.

IV. Compute Infrastructure for Data Science Research

NIST has implemented an Evaluation Management System (EMS) that will serve as the infrastructure for the DSE series. EMS integrates hardware and software components for easy deployment and reconfiguration of computational needs and enables integration of compute- and data-intensive problems within a controlled cloud. In addition, EMS enables the collection of metrics on independently running instances as well as aggregation of overall performance metrics on the core problem. This design allows for test and evaluation (T&E) of different compute paradigms (software and model changes, such as testing a solution using MPI (Message Passing Interface) and later trying it using Go channels) as well as hardware accelerations in order to best assess how a given evaluation can be run.

The underlying cloud infrastructure accommodates concurrent execution of projects—such as experiments or evaluation—on a shared hardware while being able to separate data access, network resources, users and hardware accelerators (e.g., GPU or Phi). Applications within a given project communicate with one another and access data shared with a specific user and application.

This infrastructure supports the integration of distributed as well as parallelized computations, thus providing a flexible hardware architecture for running projects on the system. Performance metrics for individual applications, their data, network and memory usages are aggregated in order to compute per-application metrics as well as global project metrics. This enables direct comparisons between different algorithmic approaches for a given project and supports studies of hardware accelerations or comparisons of compute paradigms.

The initial emphasis of the EMS is to support NIST evaluations, leveraging a private cloud infrastructure for easy deployment. To facilitate this process, a model for abstracting the complexity of inter-evaluation components (such as ingestion, validation, scoring, report generation, and return of results to participants) enables reproducibility of given problems on different compute architectures. As the model is enhanced, encrypted point-to-point communication will be integrated to protect intellectual property and sensitive data used by the infrastructure.

NIST has integrated hardware resources within a private cloud testbed (Gigabit and Infiniband networks, Tesla GPUs, Intel Phi Coprocessors, high memory compute nodes, high storage data nodes) using a local OpenStack deployment. OpenStack is open source and provides several core components that support an expandable cloud solution:

- **Computing Engine:** Deploys and manages virtual machines and other instances to handle computing tasks
- **Network Controller:** Enables fast and managed network communications
- **Storage System:** Stores objects and files (using OpenStack) and a block storage component for user control when data access speed is essential
- **Identity Services:** Provides user management
- **Image Services:** Uses virtual copies of hard disks for deployment of new virtual machine instances
- **Telemetry Services:** Keeps a verifiable count of each user's system
- **Orchestration Component:** Supports the definition of cloud resource specifications and enables the management of infrastructure for cloud services

- **Front End:** Provides a quick glance at components running on the cloud and creates new instances
- **Application Programming Interface (API):** Enables extension of core components

Since OpenStack provides block and object storage based on commodity hardware solutions, it is possible to easily add new storage components to our local cloud as the volume of data increase. Also, OpenStack can be deployed between multiples sites where each site has its own OpenStack and storage can be configured as a single shared pool or separate pools. The use of OpenStack Swift gives access to streamed data, be it local or remote via an industry-standard RESTful HTTP API. All objects are stored with multiple copies and are replicated in as-unique-as-possible availability zones and/or regions.

Our current test bed for the EMS has Gigabit as well as an Infiniband networks, 5 compute nodes with 16 cores each, 128GB, 192 GB or 256 GB of memory, and 32 TB or 48 TB of disk per node, as well as 2 extra computes nodes with 4 Tesla C2050 and 4 Phi 5100, and 5 storage nodes with 48TB of disk per node.

This cloud infrastructure allows NIST to integrate and use different technologies, such as Apache MESOS, Docker, or Google Kubernetes Containers. It also enables the use of other compute engines such as Apache Spark or Apache Hadoop.

V. Data Science Community Building & Outreach

Because data science spans a wide range of very diverse fields (biology, forensics, finance, public health monitoring, etc.), the tendency is for researchers to work independently, often applying similar, but independently developed, data-processing tools and re-solving problems that span multiple data domains. The result of this mode of operation is an overall reduction in efficiency, delayed progress, and a lack of knowledge about cross-cutting synergies and best practices for many common classes of problems.

To address issues with this siloed approach to algorithm development, NIST aims to build a community of interest within which it is expected that many of the questions posed in the sections below will be addressed. Technical symposia with a focus on generalized problems in data science are expected outcomes of this aspect of NIST's work. Within a shared community, data scientists can more effectively collaborate, coordinating their efforts on similar classes of problems.

There are already several successful examples of existing NIST programs, within which community-wide mechanisms are in place (such as symposia) for technology development, assessment, and cross-community discussion. One such example is the Text Retrieval Conference (TREC) [6], which has been held at NIST annually since 1992. This research program includes an evaluation series where researchers are able to share ideas and to compare their approaches with those of other community members by participating in shared tasks defined within tracks.

As a starting point, in March of 2014, NIST held the first Data Science Symposium [7], at which data scientists had the opportunity to discuss data science benchmarking and performance measurement, datasets and use cases for data science research, and challenges and gaps in data science technologies. There were over 700 registrants from the data science community—spanning multiple fields—with several dozen paper and poster presentations and breakout groups on topics related to data science, e.g., human-computer interaction, manufacturing, and meta-data.

It was at this symposium that many of the challenges and expected breakthroughs presented below were brought to the fore, and researchers in a range of different fields began to discuss best practices for development and assessment of data science algorithms. The next symposium for the DSRP will be held at NIST in winter of 2016, where researchers participating in the traffic pre-pilot will have the opportunity to evaluate the effectiveness of their algorithms on traffic incident detection and traffic prediction tasks.

It is expected that the new DSRP will leverage lessons learned in the initial pre-pilot to move forward effectively on a range of issues that carry across different domains (e.g., biology vs. finance), across different modalities (e.g., video data vs. structured reports), and for commonly occurring data-related tasks (e.g., anomaly detection and data cleaning).

VI. Where are the Important Future Breakthroughs?

To support the DSRP, a significant effort will be put toward investigation of the basic premises underlying data science, including big data, as well as a focus on the types of future breakthroughs that are expected. Four V's are often cited to illustrate the challenges and the need for breakthroughs in this field: Volume, Velocity, Variety, and Veracity.[8] The earliest formulation by Douglas Laney [8] included only the first three, briefly summarized below:

- Volume: Vast amounts of data generated from multiple sources, often too large to store or analyze using traditional database approaches.
- Velocity: Speed at which the massive data are being produced and collected, making it a challenge for real-time processing.
- Variety: Diverse and potentially incompatible data types

[6] http://trec.nist.gov

[7] http://www.nist.gov/itl/iad/data-science-symposium-2014.cfm

[8] A fifth V that has been proposed is Value [6], i.e., the degree to which the worth of the data is conveyed. Providing a means to visualize data can increase understandability and accessibility in ways that would otherwise be impossible, thus clarifying the underlying value of the data. In the scope of this paper Value is considered to cross-cut several data science challenges, most notably a sixth V proposed by McNulty [7] (Visualization), which we address separately as a next generation challenge.

and formats coming from multiple sources.[9]

Veracity is a fourth V, attributed to researchers at IBM [9]:

- Veracity: Quality and trustworthiness of data, given the variety of sources and degree of accuracy.

Of these four V's, the first (Volume) and second (Velocity) are critical for processing of big data. These are important aspects of the DSRP, both for the initial traffic use case where (ultimately) traffic monitoring may lead to realtime data sets (including issues of latency) and for new tracks involving very large data that one might find, e.g., in the biological domain. The third (Variety) and fourth (Veracity) encompass a wide range of next generation challenges within which algorithmic breakthroughs are critical for the advancement of data science, as will be described in the section below.

Variety, frequently referred to as *heterogeneity* [10], [11], is central to building web-scale systems for tasks such as entity resolution [12], [13]. Data diversity is a consideration for all sizes of data, not just large datasets. Indeed, a critical area of measurement science within the new DSE series is that of measuring the ability of an algorithm to analyze, assimilate, adapt, and/or fuse diverse data types.

Veracity is also a critical challenge faced by many data scientists, as the algorithms they develop are expected to apply to a wide range of diverse inputs, including data that are errorful, noisy, and inconsistent across different inputs.

The emergence of data science and the challenges associated with the four V's above are accompanied by technological progress leading to:[10]

- Massively scalable processing and storage
- Pay-as-you-go processing and storage
- Flexible schema on read vs. schema on write[11]
- Easier integration of data retrieval and analysis
- Well-supported interfaces between various domain specific languages/tools.
- Open source ecosystem during innovation[12]
- Increased bandwidth, network access, speed, and reduced latency.

The ability of data-science algorithms to address the four V's—and the provision of a methodology for assessment corresponding to challenges within these—is critical now more than ever before in light of changes such as those above.

VII. Next Generation Data Science Challenges

Several areas of data science merit an extended, in-depth study, requiring input from the research community, and aligned with next generation challenges. Table I presents some key challenges, each with a representative set of examples. The table also presents a set of traffic-related use cases, in line with the focus of the pre-pilot study mentioned in Section II. These key challenges are described in more detail below.

Provenance. Where does each piece of data come from and is that data still up to date [24]? In the context of database systems and queries, provenance refers to the ability to determine the origin of the data, or which tuples of which original databases were used (and how they were used) to produce each tuple in subsequent databases resulting from database queries [25], [26]. More generally, data provenance involves being able to determine where the data came from and the processes through which this data was derived from its original sources [27].

Data heterogeneity. How does one process data from multiple, large heterogeneous datasets? Data heterogeneity refers to different representations of the same real-world object. The differences may be structural or semantic [16].

Real time and predictive analytics. How can trends be identified and distinguished from random fluctuation in order to provide a calibrated forecast of future values. How can this be executed in real time [28]? Further, is it possible to effectively trade-off between execution time and accuracy? Predictive analytics refers to the extraction of information from data to estimate future outcomes and trends.

Knowledge assimilation and reasoning from data. How might algorithms reason with data, e.g., inferring causality [24], [29]? Knowledge assimilation and reasoning refers to understanding new data in terms of information available in an already-existing dataset, and applying the necessary processing to reflect the expert's view of the domain.

Big data replicability. How is reproducibility of data science experiments ensured, especially given that the truth may be hard to find among millions of data points where there is lots of room for error [19]? Big data replicability refers to the ability to repeat results across studies where the same research question is being asked on the same dataset.

Visualization of data. How might one visually represent data, whether in a raw form or after post-processing by any number of algorithms? Visualization refers to use of visual metaphors (boxes, groups, lines, etc.) that serve as building blocks for displaying complex data representations (e.g., spatiotemporal network analysis [30]), each with their own constraints in the amount and type of data to be displayed [31]. The integration of visualization into data science activities aids in the analysis of vast volumes of information [32], may increase efficiency [33], and may reduce user errors [20].

Data uncertainty. How might one handle quality issues due to untrustworthy or inaccurate data? Data uncertainty refers to gaps in knowledge due to inconsistency, incompleteness, ambiguities, and model approximations.

[9] Variability is a seventh V that has been proposed [7]—distinct from the notion of Variety. The former refers to the degree to which the meaning behind data can change according to time and context; the latter refers to the degree to which data formats differ from each other, according to the domain and level of formality (e.g., structured vs. unstructured). We consider Variability to be a challenge to be addressed in different ways across domains rather than a challenge that might be more broadly addressed by techniques that carry across different areas of data science.

[10] This list of areas in which technological progress has been made is an augmented version of those presented recently by Franklin [14].

[11] Flexible schema on read is an approach that allows data to be parsed at read time, rather than requiring pre-formatting prior to loading the data. Schema on write refers to prescriptive data modeling where database schema are statically defined prior to reading the data.

[12] An "ecosystem" of service providers combined with open source development allows easier sharing of applications, cross-sector use of the same components (smart homes, city services, etc.), and exchange and re-use of applications and components.

TABLE I
NEXT GENERATION CHALLENGES IN THE FIELD OF DATA SCIENCE

Challenge	Relevant Questions	Examples	Traffic Use Case
Provenance	Where did the raw data originate? Is it current? What processes were applied through which the data was derived from its original sources?	A genome sequence dataset may be recreated from raw data and the provenance records associated with genomic annotations [15].	The time of a traffic accident may be determined from traffic incident reports and provenance records associated with video data that has been cleaned and aligned with the reports.
Data Heterogeneity	How to use data from multiple large heterogeneous datasets?	A publisher may be represented either as a publication-producing entity, or as an attribute of a publication [16].	A vehicle may be represented visually in video data and descriptively in an incident report.
Predictive Analytics	How can trends be identified and distinguished from random fluctuation in order to provide a calibrated forecast of future value?	Stock market events may be forecasted from sentiments expressed in social media [17].	Future traffic patterns may be guessed from weather, imagery, and historical traffic data.
Knowledge Assimilation	How might algorithms understand new data, e.g., inferring causality from the data or accommodating real-time inference retraction?	Fraudulent activity may be inferred from (potentially altered) digital and physical data representations of known entities and events [18].	A traffic accident may be detected from the position of two cars in a video clip.
Big Data Replicability	How to reproduce experimental findings given that truth may be hard to find, consistently?	Using the same (usually massive) genomic dataset in two different studies to find genetic contributions to a particular disease may yield different results [19].	Using historical data from weather reports, traffic incident data, and traffic video data to detect an incident may yield different results.
Visualization of Knowledge	How to visually represent knowledge for decision making?	Intrusion detection systems often utilize dashboards to reflect network status and to alert security administrators of suspicious activity [20].	Visualization may be used to communicate traffic flow and accidents.
Data Uncertainty	How to handle gaps in knowledge due to the potential for untrustworthy or inaccurate data?	In RFID (radio-frequency identification) Data Management, raw antenna readings are frequently missed or tags are read by two adjacent antennas [21].	Uncertainty may arise from the lack of data available from points that occur between traffic detectors.
Mitigating Error propagation	How can algorithms mitigate cascading of error through data processing steps?	In Geographic Information Systems (GISs) inaccuracies may propagate and cascade from one layer to another, resulting in an erroneous solution to the GIS problem [22].	Errors associated with cleaning of traffic incident reports may propagate to incident detection and traffic prediction tasks.
Managing Privacy and Security	How to manage data and develop algorithms in the face of privacy and concerns/policies?	Model checking to verify that HIPAA (the federal Health Insurance Portability and Accountability Act) is being followed [23].	— (Privacy and security are not a focus in the traffic domain given the minimally restricted, or unrestricted, nature of traffic and weather data.)

Propagation and cascading of error: How might algorithms be written to mitigate propagation and cascading of error(s)? Error propagation and cascading refers to situations where one error leads to another or where a solution is skewed when imprecise or inaccurate information is combined into multiple layers [22].

Data privacy and security. How does one manage data and develop algorithms for processing data in the face of privacy and security concerns? Data privacy and security refers to the challenge of providing effective approaches for secure management of distributed data and data sharing, including those that may contain personally-identifiable information (PII). Detection of PII for anonymization purposes [34] and structural diversification for protecting privacy [35] are particularly important problems to be addressed. Other critical areas include management of access, sharing and distributability (e.g., data specific tools, metadata).

These are important challenges that cut across multiple areas of data science. There may be common algorithmic approaches and evaluation metrics associated with each of these challenges. Community input garnered within the DSRP will bring forth new insights to address cross-cutting issues pertaining to the data itself and measures associated with approaches to processing data.

The next section presents a set of representative classes of data science problems, setting the stage for defining measures to assess data science technologies within the DSRP.

VIII. CLASSES OF DATA SCIENCE PROBLEMS

This section examines several classes of problems for which techniques might be developed and evaluated across different domains, and defines representative classes of problems accompanied by examples from the planned use case of traffic incident detection and prediction, although the problem classes are broader than this single use case. Different categories of algorithms and techniques in data science will be examined, with an eye toward building an assessment methodology for the DSRP that covers each category.

Detection. Detection aims to find data of interest (often an anomaly or outlier—see Anomaly Detection below) in a given dataset. In the traffic domain, incidents are of interest, e.g., "traffic incident detection" is an important sub-problem of the traffic use case. Yang, Kalpakis, and Biem [36] analyze traffic flow in order to detect traffic incidents.

Anomaly detection. Anomaly detection is the identification of previously unseen system states that force additional pattern classes into a model. Relatedly, outlier detection is associated with identifying erroneous data items that force changes in prediction models ("influential observations"). In the traffic case, an incident may be seen as an anomaly relative to data representing free-flowing traffic. Detection of incidents in traffic data with incident and non-incident data may also be seen as system state identification and estimation.

Cleaning. Cleaning refers to the elimination of errors, omissions, and inconsistencies in data or across datasets. In the traffic use case, cleaning might involve the identification and elimination of errors in dirty traffic detector data.

Alignment. Alignment refers to the process of relating different instances of the same object [37], e.g., a word with the corresponding visual object, or time stamps associated with two different time series.[13] In the traffic use case, this might involve aligning traffic camera video and traffic incident reports.

Data Fusion. Fusion refers to the integration of different representations of the same real-world object, encoded (typically) in a well-defined knowledge base of entity types [11]. In the traffic use case, fusion might be applied to bring together a video representation of a vehicle with a description of the same vehicle in an incident report.

Identification and classification. Identification and classification attempts to determine, for each item of interest, the type or class to which the item belongs [39]. In the traffic use case, the type of incident may be critical, e.g., slipping off the road, or stopping for an extended period of time (as in bumper-to-bumper traffic).

Regression. Regression refers to the process of finding functional relationships between variables. In our pilot traffic flow prediction challenge, we wish to predict traffic speed using covariates including flow volume, percentage occupancy, and training sets of past multivariate time series.

Prediction. Prediction refers to the estimation of a variable or multiple variables of interest at future times. In our traffic pilot, we might pose the challenge of predicting traffic flow rate as a function of other variables.

Structured prediction. Structured prediction refers to tasks where the outputs are structured objects, rather than numeric values [40], [41]. This is a desirable technique when one wishes to classify a variable in terms of a more complicated structure than producing discrete or real-number values. In the traffic domain an example might be producing a complete road network where only some of the roads are observed.

Knowledge base construction. Knowledge base construction refers to the construction of a database that has a predefined schema, based on any number of diverse inputs. Researchers have developed many tools and techniques for Automated Knowledge Base Construction (AKBC)[14]. In the traffic use case a database of incidents and accidents could be constructed from news reports, time-stamped GPS coordinates, historical traffic data, imagery, etc.

Density estimation. Density estimation refers to the production of a probability density (or distribution function), rather than a label or a value [42], [43]. In the traffic use case, this might involve giving a probability distribution of accidents happening over a given time interval.

Joint inference. Joint inference refers to joint optimization of predictors for different sub-problems using constraints that enforce global consistency. Joint inference may be used for detection and cleaning to arrive at more accurate results [44]. In the traffic use case, weather conditions may act as a constraint on traffic incident detection outcomes, while at the same time, traffic incident detection may act as a constraint on weather conditions during time periods where weather data may not be available.

Other classes of problems. Data science problems may involve ranking, clustering, and transcription (alternatively called "structured prediction" as defined above). Several of these are described by Bengio et al. [45]. Additional classes of problems rely on algorithms and techniques that apply to raw data at an earlier "preprocessing" stage.

Given the broad scope of the classes of problems above, a number of different data processing algorithms and techniques may be employed for which an evaluation methodology is essential, e.g., for benchmarking. The next section elaborates on the range of methodologies needed for measuring technology effectiveness within the new DSRP.

IX. Methodologies for Measuring Effectiveness of Data Science Technologies

This section examines a range of different questions for the development of assessment methodologies, divided broadly into three categories: (1) aspects of data science measurement; (2) how to pursue data science without compromising privacy; and (3) how to preserve and distribute data and software. These questions set the stage for the new DSRP, addressing some of the most critical issues and areas of inquiry for data science.

A. Aspects of Data Science Measurement

1) How does one measure accuracy when all truth data are not annotated fully?: Ground truth may be prohibitively expensive or laborious to obtain in cases where human-labeled data are needed. In some cases, ground truth may be entirely "unobtainable," where the true answer is not known. For most predictive tasks, ground truth data become available when realtime datasets or future data materialize (e.g., accident prediction in video). For non-predictive tasks (e.g., detection of traffic incidents), Katariya et al.'s [46] work on active evaluation of classifiers estimates accuracy based on a small labeled set and human labeler. Some NIST evaluations (TREC, [47]) apply accuracy measures that accommodate the lack of full truth data, often employing mediated adjudication approaches (e.g., pooling relevance assessments of participants in the evaluation to approximate recall). Another potential approach is to use simulated data as a proxy for ground truth.

[13] Data alignment is frequently used for entity resolution, which is identifying common entities among different data sources. Getoor and Machanavajjhala [12] and Christen [38] are two works that describe entity resolution techniques.

[14] 4th Workshop on Automated Knowledge Base Construction http://www.akbc.ws/2014/

Within the DSRP, these and other approaches for addressing issues concerning ground-truth metadata will be explored.

2) How does one measure data assimilation?: Data assimilation—a process by which observations are incorporated into a computer model of a real system—addresses the problem of not knowing the initial conditions of a given system [48]. Using current and past limited available observations and short range forecasts, data assimilation analyzes the data to estimate the background of the observed system and produces the best estimate of the initial conditions of the forecast system. The better the estimate, the more accurate the forecast [49].

While assimilation and fusion are similar in nature, there are differences: assimilation refers to modeling observations of the same objects (in situ, remotely, etc.) from sensors of different types, whereas fusion refers to bringing together different datasets to arrive at a result or response. Within the DSRP, both assimilation and fusion are assumed to be central to data science measurement.

3) How does one measure knowledge representation through Visualization of data?: The Visualization Analytics Science & Technology community has developed a "VAST Challenge," run annually for the past 3 years[15], for assessment of visual analytics applications for both large scale situation analysis and cyber security. Topics of importance for the DSRP include automatic graph analysis and best practices for combined and multimodal datasets. Several different approaches to developing and assessing information visualization for very large datasets have been implemented [50], [51]. Visualization paradigms are often assessed by the number of data points and the level of granularity represented [52] and by types of relationships that can be represented [31].

4) How does one develop sound benchmark measurements that satisfactorily convey system performance?: Sound benchmarking requires the integration of a variety of research areas: the mathematics of designing good benchmark metrics, the systems research of implementing monitors that collect the data with minimal overhead, and the understanding of the field in choosing representative workflows to measure the performance of different computer systems [53], [54]. As computer systems change and needs change, the desired workflows need to be changed. Within the DSRP, the use of program-agnostic metrics and software performance monitors that can run on a variety of hardware architectures will enable the application of benchmark metrics and monitors in future workflows on different software and hardware architectures.

5) How does one measure the effectiveness of each data characteristic for making decisions or formulating knowledge?: Principal Component Analysis and other dimensionality reduction techniques give some indication of the dimensions of variation present in the data. Various feature selection approaches may be applied to better understand the contribution of data characteristics for decision making and knowledge formulation [55]. As a clarifying example, in the traffic domain within the DSRP, a task would be to determine how much lane detector, weather, and accident data contribute to the ability to perform the overall tasks of traffic incident detection and traffic prediction.

B. How does one pursue data science without compromising privacy?

Collection and sharing strategies are needed so that researchers are able to run experiments on the same data, with minimal barriers. For example, the traffic and weather data in our pilot DSE evaluation are open and easily distributable. However, the DSRP will include a wide range of domains (multiple tracks) and thus will need to keep track of what can and cannot be shared and under what conditions. Personally Identifiable Information (PII) or, by fusion, merging multiple datasets that bring PII into the composite result, cannot be shared. In cases where PII data are needed, it is important to determine the feasibility of *data construction*—but the scale may not be as large as it would be for "data in the wild." Recent conferences that have included privacy as a central topic, e.g., SIAM International Conference on Data Mining [56] and some that have focused entirely on this issue (e.g., the Big Data Privacy Workshop [57]).

C. How does one preserve data and software used for data science?

In the field of Natural Language Processing, researchers rely heavily on the University of Pennsylvania's Linguistic Data Consortium (LDC), which collects, creates, annotates, and distributes data, ensuring that all materials are carefully managed, with lawyers verifying copyright and other issues (e.g., licensing). Other organizations serve a similar role as the LDC, but are geared toward more data science, e.g., Research Data Alliance and Data.gov. In addition, NIST is working on data preservation and archival (i.e., keeping bits around forever) and tracing the history of data [58]–[60].

X. Concluding Remarks: IAD's Role for Data Science

This paper lays out the foundation of IAD's newly formed Data Science Research Program and describes IAD's role in the future of the data science discipline. Classes of data science problems and next generation data science challenges as well as areas of important future breakthroughs are discussed. An overview of evaluation and metrology, standards, computing infrastructure needs, and methodologies for measuring effectiveness of data science technologies is presented.

IAD's role for meeting the measurement challenges for data science has four primary facets. These include developing measures for assessment, establishing standards, forming working groups consisting of researchers in the community, and deploying a sound framework for evaluating technology effectiveness.

In addition, IAD aims to build a community of interest within which it is expected that many of the questions posed

[15] The latest (2015) VAST Challenge information can be found at: http://vacommunity.org/VAST+Challenge+2015

in this paper will be addressed. Technical symposia with a focus on generalized problems in data science are expected outcomes of this aspect of NIST's work.

Additionally, it is expected that agile system architectures, system benchmarking tools, and novel approaches will emerge from the development of technologies that are evaluated in the DSE series.

Finally, the DSE series will be organized each year by NIST, in coordination with the data science research community, for the assessment of technologies for big data and data science analytics. NIST will serve the community in providing relevant datasets, metrics, tasks, protocols, and analysis tools.

Disclaimer:

These results are not to be construed or represented as endorsements of any participants system, methods, or commercial product, or as official findings on the part of NIST or the U.S. Government.

Certain commercial equipment, instruments, software, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the equipment, instruments, software or materials are necessarily the best available for the purpose.

References

[1] M. Smith, "The White House names Dr. D.J. Patil as the first U.S. chief data scientist," Feb 2015. [Online]. Available: https://www.whitehouse.gov/blog/2015/02/18/white-house-names-dr-dj-patil-first-us-chief-data-scientist

[2] L. Cao, H. Motoda, G. Karypis, and B. Boethals, "DSAA trends and controversies," in *International Conference on Data Science and Advanced Analytics (DSAA)*, Shanghai, 2014.

[3] W. Chang, "1st ISO/IEC JTC 1 study group on big data meeting." [Online]. Available: http://jtc1bigdatasg.nist.gov/

[4] ——, "NIST special publication 1500-6 information technology laboratory: DRAFT NIST big data interoperability framework: Volume 6, reference architecture."

[5] ——, "NIST big data public working group (NBD-PWG) request for public comment," 2015. [Online]. Available: http://bigdatawg.nist.gov/V1_output_docs.php

[6] B. Marr, "Why only one of the 5 Vs of big data really matters," 2015. [Online]. Available: http://www.ibmbigdatahub.com/blog/why-only-one-5-vs-big-data-really-matters

[7] E. McNulty, "Understanding big data," *Dataconomy*, 2014. [Online]. Available: dataconomy.com/seven-vs-big-data/

[8] D. Laney, "3D data management: Controlling data volume, velocity, variety," Feb. 2001. [Online]. Available: http://blogs.gartner.com/doug-laney/deja-vvvue-others-claiming-gartners-volume-velocity-variety-construct-for-big-data/

[9] IBM, "The four V's of big data," 2013. [Online]. Available: http://www.ibmbigdatahub.com/infographic/four-vs-big-data

[10] C. A. Knoblock and P. Szekely, "Exploiting semantics for big data integration," *AI Magazine*, vol. 36, no. 1, pp. 25–38, 2015.

[11] J. Sleeman, T. Finin, and A. Joshi, "Entity type recognition for heterogeneous semantic graphs," in *2013 AAAI Fall Symposium Series*, 2013.

[12] L. Getoor and A. Machanavajjhala, "Entity resolution: theory, practice & open challenges," *Proceedings of the VLDB Endowment*, vol. 5, no. 12, pp. 2018–2019, 2012.

[13] J. Pujara, H. Miao, L. Getoor, and W. W. Cohen, "Using semantics & statistics to turn data into knowledge," *AI Magazine*, vol. 36, no. 1, pp. 65–74, 2015.

[14] M. Franklin, "Big data and data science: Some hype but real opportunities," University of Florida, Mar. 2015. [Online]. Available: https://www.cise.ufl.edu/content/uf-informatics-institute-inaugural-symposium

[15] S. S. Morrison, R. Pyzh, M. S. Jeon, C. Amaro, F. J. Roig, C. Baker-Austin, J. D. Oliver, and C. J. Gibas, "Impact of analytic provenance in genome analysis," *BMC Genomics*, vol. 15, no. Suppl 8: S1, 2014.

[16] D. George, "Understanding structural and semantic heterogeneity in the context of database schema integration," *Journal of the Department of Computing*, no. 4, 2005.

[17] A. Mittal and A. Goel, "Stock prediction using twitter sentiment analysis," 2011.

[18] D. Doermann, "Visual media forensics: Knowing when seeing is believing," University of Florida, mar 2015. [Online]. Available: https://www.cise.ufl.edu/content/uf-informatics-institute-inaugural-symposium

[19] T. H. Saey, "Big data studies come with replication challenges," *Science News*, vol. 187, no. 3, pp. 22–27, 2015.

[20] S. Few, *Information Dashboard Design: Displaying Data for At-a-glance Monitoring*. Analytics Press, 2013.

[21] D. Suciu, D. Olteanu, C. Ré, and C. Koch, "Probabilistic databases," *Synthesis Lectures on Data Management*, vol. 3, no. 2, pp. 1–180, 2011.

[22] K. E. Foote, "The Geographer's craft project," 2015. [Online]. Available: http://www.colorado.edu/geography/gcraft/contents.html

[23] A. Datta, "Privacy through accountability: A computer science perspective," in *Distributed Computing and Internet Technology*. Springer, 2014, pp. 43–49.

[24] A. Meliou, W. Gatterbauer, and D. Suciu, "Bringing provenance to its full potential using causal reasoning." in *Theory and Practice of Provenance*, 2011.

[25] P. Buneman, S. Khanna, and W.-C. Tan, "Data provenance: Some basic issues," in *FST TCS 2000: Foundations of Software Technology and Theoretical Computer Science*, ser. Lecture Notes in Computer Science, S. Kapoor and S. Prasad, Eds. Springer Berlin Heidelberg, 2000, vol. 1974, pp. 87–93.

[26] L. C. James Cheney and W.-C. Tan, "Provenance in databases: Why, how, and where," *Foundations and Trends in Databases*, vol. 1, no. 4, pp. 379–474, 2007.

[27] Y. L. Simmhan, B. Plale, and D. Gannon, "A survey of data provenance in e-science," *SIGMOD Rec.*, vol. 34, no. 3, pp. 31–36, Sep. 2005.

[28] S. Finlay, *Predictive Analytics, Data Mining and Big Data: Myths, Misconceptions and Methods*. Palgrave Macmillan, 2014.

[29] J. Pearl, "Causal inference in statistics: An overview," *Statistics Surveys*, vol. 3, pp. 96–146, 2009.

[30] J. Gelernter and K. M. Carley, "Spatiotemporal network analysis and visualization," *International Journal of Applied Geospatial Research*, vol. 6, no. 2, pp. 77–97, 2015.

[31] I. Meirelles, *Design for Information: An Introduction to the Histories, Theories, and Best Practices Behind Effective Information Visualizations*. Rockport Publishers, 2013.

[32] D. A. Keim, "Information visualization and visual data mining," *Visualization and Computer Graphics, IEEE Transactions on*, vol. 8, no. 1, pp. 1–8, 2002.

[33] U. Fayyad, A. Wierse, and G. Grinstein, *Information Visualization in Data Mining and Knowledge Discovery*, ser. The Morgan Kaufmann series in data management systems. Morgan Kaufmann, 2002.

[34] C. Li, C. Aggarwal, and J. Wang, "On anonymization of multi-graphs," in *Proceedings of the 2011 SIAM International Conference on Data Mining*, ser. Proceedings. Society for Industrial and Applied Mathematics, Apr. 2011, pp. 711–722.

[35] C.-H. Tai, S. Y. Philip, D.-N. Yang, and M.-S. Chen, "Structural diversity for privacy in publishing social networks," in *Proceedings of the 2011 SIAM International Conference on Data Mining*, B. Liu, H. Liu, C. Clifton, T. Washio, and C. Kamath, Eds. Philadelphia, PA: Society for Industrial and Applied Mathematics, Apr. 2011, pp. 35–46.

[36] S. Yang, K. Kalpakis, and A. Biem, "Detecting road traffic events by coupling multiple timeseries with a nonparametric bayesian method," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 5, pp. 1936–1946, Oct. 2014.

[37] R. Fagin, L. Haas, M. Hernández, R. J. Miller, L. Popa, and Y. Velegrakis, *Conceptual Modeling: Foundations and Applications*. Springer, 2009.

[38] P. Christen, *Data Matching: Concepts and Techniques for Record Linkage, Entity Resolution, and Duplicate Detection*, ser. Data-Centric

Systems and Applications. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[39] M. Jeevan, "Fundamental methods of data science: Classification, regression and similarity matching," Jan. 2015. [Online]. Available: http://www.kdnuggets.com/2015/01/fundamental-methods-data-science-classification-regression-similarity-matching.html

[40] G. H. Bakir, T. Hofmann, B. Schlkopf, A. J. Smola, B. Taskar, and S. V. N. Vishwanathan, Eds., *Predicting Structured Data (Neural Information Processing)*. The MIT Press, 2007.

[41] J. D. Lafferty, A. McCallum, and F. C. N. Pereira, "Conditional random fields: Probabilistic models for segmenting and labeling sequence data," in *Proceedings of the Eighteenth International Conference on Machine Learning*, ser. ICML '01. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2001, pp. 282–289.

[42] E. Fix and J. Hodges, J. L., "Discriminatory analysis. nonparametric discrimination: Consistency properties," *International Statistical Review / Revue Internationale de Statistique*, no. 3, pp. pp. 238–247, 1957.

[43] B. W. Silverman and M. C. Jones, "An important contribution to nonparametric discriminant analysis and density estimation: Commentary on Fix and Hodges (1951)," *International Statistical Review / Revue Internationale de Statistique*, vol. 57, no. 3, pp. pp. 233–238, 1989.

[44] C. Mayfield, J. Neville, and S. Prabhakar, "A statistical method for integrated data cleaning and imputation," Purdue University, Tech. Rep. 09-008, Sep. 2009.

[45] Y. Bengio, I. J. Goodfellow, and A. Courville, "Deep learning," 2015. [Online]. Available: http://www.iro.umontreal.ca/bengioy/dlbook

[46] N. Katariya, A. Iyer, and S. Sarawagi, "Active evaluation of classifiers on large datasets," in *2013 IEEE 13th International Conference on Data Mining*, vol. 0. Los Alamitos, CA, USA: IEEE Computer Society, 2012, pp. 329–338.

[47] "Text retrieval conference," 2014. [Online]. Available: http://trec.nist.gov

[48] E. Kalnay, *Atmospheric Modeling, Data Assimilation and Predictability*, 1st ed. New York: Cambridge University Press, Dec. 2002.

[49] O. Talagrand, "Assimilation of observations: An introduction," *Meteorological Society of Japan Series 2*, vol. 75, pp. 81–99, 1997.

[50] C. Ware, *Information Visualization, Third Edition: Perception for Design*, 3rd ed. Waltham, MA: Morgan Kaufmann, Jun. 2012.

[51] B. B. Bederson and B. Shneiderman, *The Craft of Information Visualization: Readings and Reflections*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2003.

[52] R. Marty, *Applied security visualization*. Addison-Wesley Upper Saddle River, 2009.

[53] R. Jain, *The Art Of Computer Systems Performance Analysis: Techniques For Experimental Design, Measurement*. John Wiley & Sons, 1991.

[54] J. C. De Kergommeaux, E. Maillet, and J. Vincent, "Monitoring parallel programs for performance tuning in cluster environments," *Parallel Program Development for Cluster Computing: Methodology, Tools and Integrated Environments" book, P. Kacsuk and JC Cunha eds*, 2001.

[55] I. Guyon and A. Elisseeff, "An introduction to variable and feature selection," *The Journal of Machine Learning Research*, vol. 3, pp. 1157–1182, 2003.

[56] M. Zaki, Z. Obradovic, P. N. Tan, A. Banerjee, C. Kamath, and S. Parthasarathy, Eds., *Proceedings of the 2014 SIAM International Conference on Data Mining*. Society for Industrial and Applied Mathematics, 2014.

[57] "Big data privacy workshop: Advancing the state of the art in technology and practice," 2014. [Online]. Available: http://web.mit.edu/bigdata-priv/

[58] W. Allasia, W. Bailer, S. Gordea, and W. Chang, "A novel metadata standard for multimedia preservation," *Proceedings of iPres*, 2014.

[59] W. Chang, "Preliminary digital preservation interoperability framework (dpif) results," in *Archiving Conference*, vol. 2010, no. 1. Society for Imaging Science and Technology, 2010, pp. 202–202.

[60] ——, "Advanced digital image preservation data management architecture," in *Archiving Conference*, vol. 2009, no. 1. Society for Imaging Science and Technology, 2009, pp. 178–182.

Precision Spectroscopy to Enable Traceable Dynamic Measurements of Pressure

Zeeshan Ahmed, Douglass Olson, Kevin O. Douglass
Sensor Science Division, National Institute of Standards and Technology 100 Bureau Dr, Gaithersburg MD 20899
Author e-mail address: kevin.douglass@nist.gov

Abstract: We present recent work aimed at creating a standard for the dynamic measurement of pressure. A near-IR laser spectroscopy system is demonstrated for measuring 8 cm^{-1} in 50 µs with a 4 kHz repetition rate.

OCIS codes: (300.1030) Spectroscopy Absorption; (000.0000), (300.6340) Spectroscopy, infrared, (300.6260) Spectroscopy, diode lasers

1. Introduction

Dynamic measurements of pressure are ubiquitous to modern life for example they are used for refining the efficiency internal combustion engines where the pressure cycles can reach 10 MPa at rates of tens of kilohertz.[1] High speed dynamic pressure sensors are used in automobiles to detect impacts in order to determine if the airbags should be deployed. Dynamic pressure mapping is used to understand the forces exerted on a dummy during crash test for automotive safety.[2] Another area of critical safety importance is characterizing the concussion inducing blast waves encountered on a battlefield which typically have a peak pressure near 1 MPa with duration of tens microseconds. However, even with the vast importance of dynamic measurements of pressure on a diverse cross-section of industry there lacks a traceable calibration to nationally (or internationally) recognized standard. Currently no National Metrology Institute (NMI) offers calibration services for these dynamic measurements at the needed measurement rates which is on the order of tens of kilohertz. Our goal is to develop traceability using high speed precision spectroscopy to measure the pressure broadened linewidth and temperature induced intensity changes at a measurement rate near one hundred kilohertz with uncertainties of 5 % or less.

Whenever there is an adiabatic change in pressure there is a corresponding change in temperature and so any dynamic measurement of pressure must also include a dynamic measurement of temperature because of the temperature dependence of the molecular lineshape. Typically, spectroscopic measurements of temperature use the ratio of the intensities of two ro-vibrational transitions from the same vibrational band but with different ground state energies and or temperature sensitivities. As an alternative to this two-line approach we propose scanning over many transitions and then perform a multi-spectrum fit for pressure, temperature, intensity with fixed mole fraction. To achieve rapid and broad wavelength tuning we are leveraging the well-known temperature dependence of the lasing frequency in common distributed feedback (DFB) lasers. Sanders et al. have demonstrated nearly 20 cm^{-1} scanning at a one kilohertz rate by using a chopped external laser to heat the laser substrate.[3] By applying a 2 ampere 250 ns duration current pulse directly to the DFB Njegovec et al has demonstrated wavelength tuning on the order of 50 cm^{-1} in 250 ns with a 10 kHz repetition rate.[4] The wavelength tuning is driven by internal heating of the substrate due to Joule heating.

2. Experiment

In our work we built upon Njegovec et al.'s approach. A 50 µs 8 Volt pulse generated from an arbitrary function generator at a repetition rate of 4 kHz is applied as modulation to the input of a commercial diode laser controller. The peak current from the current controller is about 500 mA. The DFB is a TO-can style with internal TEC cooling unit and operates at 1571 nm (6366 cm^{-1}). The DFB is initially internally cooled to a temperature of 0 ºC. A portion of the beam is sent to a temperature controlled solid silicon etalon with an FSR of 0.017 cm^{-1} for wavelength is measurement. The etalon signal is digitized at 1 GS/s with 12-bit vertical resolution. The remaining portion of the laser beam is sent through a 1-meter-long absorption cell and the resulting signal is focused onto a 400 MHz detector low pass filtered below 100 MHz and digitized at 200 MS/s using a 16 bit DAQ. The absorption cell was filled with 46.4 kPa of CO_2. A total of 164 pulses were recorded at a rate of 4 kHz and averaged. The total acquisition time was 41 ms. The bandwidth covered in each pulse is greater than 8 cm^{-1} and bandwidths up to about 13 cm^{-1} have been measured. We demonstrate scanning from R(26e) to R(R40e) of the (30012)←(00001) vibrational band of CO_2

Douglass, Kevin; Ahmed, Zeeshan; Olson, Douglas.
"Precision Spectroscopy to Enable Traceable Dynamic Measurements of Pressure."
Paper presented at the OSA Conference on Lasers and Electro-optics (CLEO), San Jose, CA, Jun 5-Jun 10, 2016.

centered at 6348 cm^{-1}. The resulting spectrum is shown in Fig 1 overlaid with a simulation created using HITRAN 2012. [5]

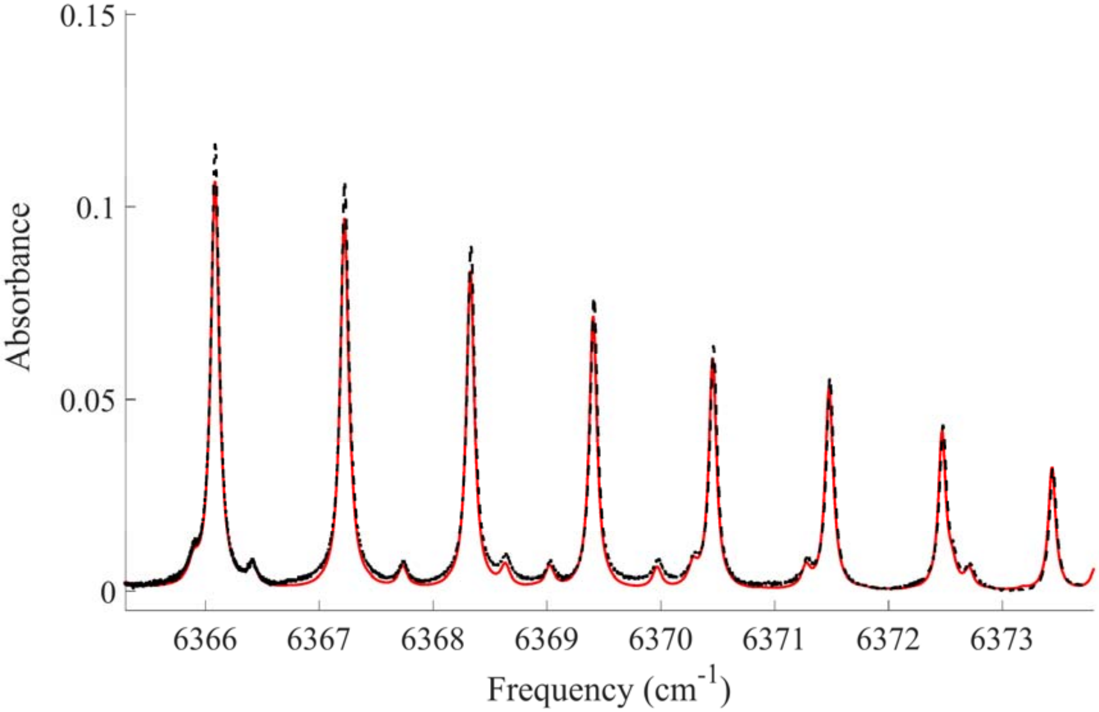


Figure 1. Absorption spectrum of CO_2 in a 1 meter path length at 46.4 kPa (black) overlaid with the simulation (red). The 8 cm^{-1} slice of the spectrum was acquired in 50 µs at rate of 4 kHz.

3. Summary

We have presented a method for using Joule heating via current pulsing to achieve rapid wavelength scanning of a DFB laser to record an 8 cm^{-1} section of the CO_2 spectrum in 50 µs with repetition rate of 4 kHz. An analysis of the spectrum of CO_2 using traditional methods compared to a multi-line fit to determine pressure and temperature is currently underway. The challenges, tradeoffs, and future directions of the rapid wavelength tuning method will be discussed. We will also present a rapid wavelength tuning in combination with wavelength modulation spectroscopy in order to achieve unprecedented speed and sensitivity.

[1] Hjelmgren, J. 2003 Dynamic Measurement of Pressure - A Literature Survey. *SP Swedish National Testing and Research Institute*. **SP Report 2002:34**.

[2] https://www.tekscan.com/.

[3] Sanders, S.T., et al. 2001 Rapid temperature tuning of a 1.4-mu m diode laser with application to high-pressure H2O absorption spectroscopy. *Optics Letters*. **26**(20): p. 1568-1570.

[4] Njegovec, M. and D. Donlagic 2013 Rapid and broad wavelength sweeping of standard telecommunication distributed feedback laser diode. *Optics Letters*. **38**(11): p. 1999-2001.

[5] Rothman, L.S., et al. 2013 The HITRAN2012 molecular spectroscopic database. *Journal of Quantitative Spectroscopy & Radiative Transfer*. **130**: p. 4-50.

“Precision Spectroscopy to Enable Traceable Dynamic Measurements of Pressure.”

Laser Refractometer as a Transfer Standard of the Pascal

Patrick Egan, Jack Stone, Jacob Ricker, and Jay Hendricks
National Institute of Standards and Technology, 100 Bureau Dr, Gaithersburg MD 20899
Email: patrick.egan@nist.gov

***Abstract*—We have developed a new low pressure sensor which is based on the measurement of (nitrogen) gas refractivity inside a Fabry–Perot (FP) cavity. We compare pressure determinations via this laser refractometer to that of well-established ultrasonic manometers throughout the range 100 Pa to 100 000 Pa. The refractometer demonstrates 10^{-6} precision for $p > 50$ kPa;—as good or better than the manometer—we argue that a laser refractometer represents a state-of-the-art transfer standard of the pascal. We also claim the refractometer has an accuracy of $U(p_{\mathrm{FP}}) = [(16\,\mathrm{mPa})^2 + (11.9\times10^{-6}\cdot p)^2]^{1/2}$, as realized through the properties of nitrogen gas.**

***Index Terms*—Fabry–Perot, length measurement, pressure measurement, refractive index, uncertainty.**

I. Introduction

During the past several years we have been developing a low pressure sensor that utilizes a laser refractometer and the ideal gas relation $p \propto (n-1)k_{\mathrm{B}}T$, where the pressure of a gas can be determined by a measure of the gas refractivity $n-1$ and thermal energy $k_{\mathrm{B}}T$ [1]. This approach is a departure from the traditional U-tube manometer where pressure $p = hg\rho$ comes from a measure of the liquid-column height h, with gravity g and the fluid density ρ being well-known [2]. Our chief motivation for this effort is ecological (that is, to move away from the toxin mercury), but we also endeavor to overcome the technical drawbacks of manometers, among which are slowness, size, sensitivity to vibration, and limited range. The metrology behind our technique is interferometry (and laser wavelength), which is used to measure the change in optical length of a Fabry–Perot (FP) cavity going from vacuum to pressure at a level of 3×10^{-10}. Our apparatus is small (about $30\,\mathrm{cm}^3$), fast and precise (1 mPa for 1 s averaging), and can hold this precision across more than five decades of pressure.

II. Method and Results

Our refractometer shown in Fig. 1 consists of two separate FP cavities built out of one piece of low thermal expansion glass; a reference cavity is permanently held at vacuum and a measurement cavity is filled with gas; the cavities have a moderate finesse of 960. The pressure of the gas in the FP cavity is measured as

$$p_{\mathrm{FP}} = \frac{1}{c_1 - d_{\mathrm{m}} - d_{\mathrm{r}}}\left(\frac{\Delta f}{\nu}\right) - \frac{c_2 - c_1 d_{\mathrm{m}}}{(c_1 - d_{\mathrm{m}} - d_{\mathrm{r}})^3}\left(\frac{\Delta f}{\nu}\right)^2 + \frac{2(c_2 - c_1 d_{\mathrm{m}})^2 - c_3(c_1 - d_{\mathrm{m}} - d_{\mathrm{r}})}{(c_1 - d_{\mathrm{m}} - d_{\mathrm{r}})^5}\left(\frac{\Delta f}{\nu}\right)^3, \quad (1)$$

where $\frac{\Delta f}{\nu}$ is the effective fractional change in cavity resonance, d_{m} and d_{r} are (compressibility) distortion terms for the measurement and reference cavities respectively. The proportionality constants

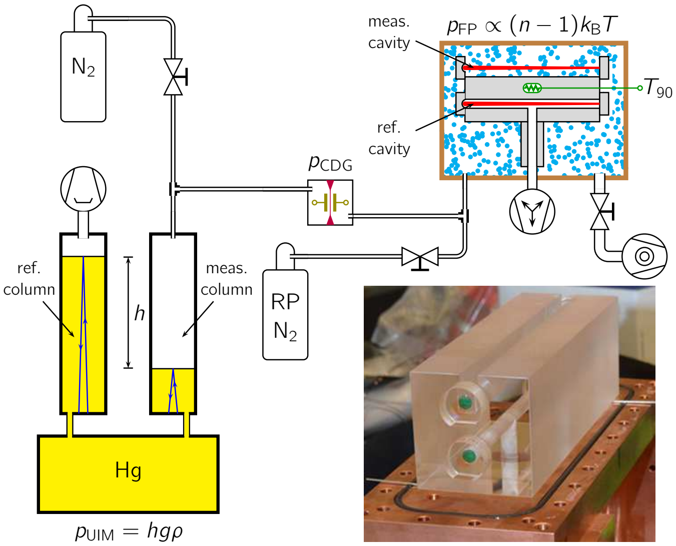


Fig. 1. Plumbing to compare a refractometer to a manometer; inset photograph of refractometer. RP, research purity; CDG, capacitance diaphragm gauge.

$$\begin{aligned} c_1 &= \frac{3}{2k_{\mathrm{B}}T}A_R \\ c_2 &= \frac{3}{8(k_{\mathrm{B}}T)^2}\left(A_R^2 - 4A_R B_p + 4B_R\right) \\ c_3 &= \frac{3}{16(k_{\mathrm{B}}T)^3}\left(5A_R^3 - 4A_R^2 B_p + 16A_R B_p^2 \right. \\ &\quad \left. + 4A_R B_R - 16B_p B_R - 8A_R C_p + 8C_R\right), \end{aligned} \quad (2)$$

are defined by the refractivity virial coefficients (A_R, B_R, and C_R), the density virial coefficients (A_p, B_p, and C_p), and the Boltzmann constant k_{B} and thermodynamic temperature T. The proportionality constants in (1) are fixed properties of the gas species which fills the cavity, and it is the terms $\frac{\Delta f}{\nu}$, d_{m}, and d_{r} that are specific to each FP cavity; these terms need to be characterized before a gas pressure can successfully be determined with a refractometer. The effective fractional change in cavity resonance $\frac{\Delta f}{\nu}$ is what is actually measured for a given change in pressure: it is an rf beat frequency between two HeNe lasers; one locked to the resonance of a reference cavity held at vacuum, and one locked to the resonance of a measurement cavity which is filled with gas; a complete definition of $\frac{\Delta f}{\nu}$ is given in Ref. [1] The distortion term d_{r} is determined by monitoring how the resonance frequency of the reference cavity changes as the exterior of the refractometer is

U.S. Government work not protected by U.S. copyright

Egan, Patrick; Stone Jr., Jack; Ricker, Jacob; Hendricks, Jay.
“Laser ReFractometer as a Transfer Standard of the Pascal.”
Paper presented at the CPEM 2016 Conference, Ottawa, Canada, Jul 10-Jul 15, 2016.

TABLE I
EXPANDED UNCERTAINTY FOR PRESSURE MEASURED BY A LASER REFRACTOMETER AT $p = 100\,\mathrm{kPa}$.

parameter	contribution to	relative $U(p_{\mathrm{FP}}) \times 10^6$	notes
$A_R = 4.44612(4)\,\mathrm{cm}^3/\mathrm{mol}$		9.0	i
$B_R = 0.9(2)\,\mathrm{cm}^6/\mathrm{mol}^2$		1.8	[4]
$C_R = -95(10)\,\mathrm{cm}^9/\mathrm{mol}^3$		0.01	[4]
$B_p = -4.02(15)\,\mathrm{cm}^3/\mathrm{mol}$		6.2	[5]
$C_p = 1434(200)\,\mathrm{cm}^6/\mathrm{mol}^2$		1.0	[5]
$T = 302.919(1)\,\mathrm{K}$		3.3	ii
$k_{\mathrm{B}} = 1.3806488(13) \times 10^{-23}\,\mathrm{JK}^{-1}$		1.8	[7]
$\frac{\Delta f}{\nu} = 2.649422(2) \times 10^{-4}$		0.5	iii,iv
$d_r = 1.092(2) \times 10^{-6}$		0.4	iv
$d_m = 9.83(5) \times 10^{-7}$		1.1	iv
gas impurity		0.7	v
compression hysteresis		1.1	vi
nonlinear length change	15 mPa		[1]
lock offsets	4 mPa		vii
anomalous distortion	1.2 mPa		viii
outgassing	1.3 mPa		ix
intercavity length drift	0.5 mPa		ix
overall uncertainty ($k = 2$)	$\left[(16\,\mathrm{mPa})^2 + (11.9 \cdot p)^2\right]^{1/2}$		

[i] Based on the most accurate measurement of nitrogen refractivity [1]—A_R is limited by how accurate the pascal can be realized.
[ii] Measured with an SPRT and includes $U(T - T_{90})$ [6].
[iii] Includes errors in the estimate of cavity length, mirror and diffraction phase shifts, and vacuum-wavelength.
[iv] These terms are specific to one of our laser refractometers. In principle, the terms are correlated with uncertainty already expressed in A_R, and their contribution to $U(p_{\mathrm{FP}})$ is smaller than what is stated.
[v] Worst-case is 0.0001 % CO_2 in 99.9999 % N_2.
[vi] Our FP cavity is made of ULE, which has notably low hysteresis.
[vii] Caused by residual amplitude modulation.
[viii] For temperature changes of 1 mK or less.
[ix] For measurements completed within 0.5 h after a fill.

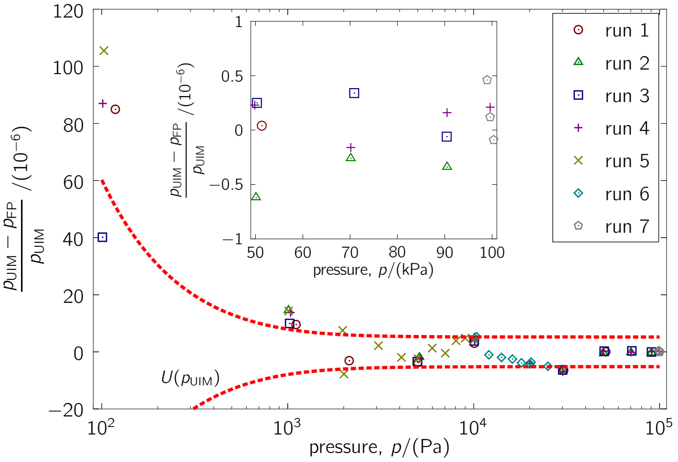


Fig. 2. Disagreement in pressure as measured by a laser refractometer (p_{FP}) and ultrasonic manometer (p_{UIM}); manometer uncertainty $U(p_{\mathrm{UIM}}) = [(6\,\mathrm{mPa})^2 + (5.2 \times 10^{-6} \cdot p)^2]^{1/2}$ also shown.

brought to pressure; the change in resonance is measured by beating the cavity resonance against a known laser frequency reference, in our case an iodine-stabilized laser. Finally, the distortion term d_{m} is determined via helium correction: we fill the measurement cavity with helium of known pressure and temperature, and calculate the theoretical refractivity; the error between the calculated refractivity and what the refractometer measures is attributed to d_{m} [3].

In the top part of Tab. I we list expanded uncertainties for all parameters in (1) and (2), and show the contribution of each parameter to the relative expanded uncertainty for a pressure determination by the refractometer at 100 kPa. It is worth noting that the chief contributor to $U(p_{\mathrm{FP}})$—A_R, the first refractivity virial coefficient—comes from a measurement of nitrogen refractivity at $p = 100.0000(6)\,\mathrm{kPa}$, $T = 302.919(1)\,\mathrm{K}$ and $\lambda_{\mathrm{vac}} = 632.9908(2)\,\mathrm{nm}$; thus, $U(p_{\mathrm{FP}})$ at this particular pressure is entirely independent of other virial coefficients. Furthermore, since we operate at the same temperature and vacuum-wavelength, a certain cancellation of errors occurs at other pressures, leading to a complicated relationship between the uncertainty of the final result and the uncertainty of the parameters in Tab. I. Also, knowledge of A_R is limited by how well nitrogen gas pressure can be measured with a manometer: if the pascal can be realized more accurately than current means, the more accurate measurements of A_R would correspondingly reduce $U(p_{\mathrm{FP}})$. In addition to the uncertainties in the parameters of (1) and (2), there are experimental limitations, as listed in the bottom part of Tab. I. These limitations end up dominating $U(p_{\mathrm{FP}})$ at lower pressures because they are responsible for an offset term in the refractometer (a pressure independent error).

In Fig. 2 we show pressure measurements using the laser refractometer as compared to NIST's ultrasonic mercury manometer, one of the world's most accurate realizations of the pascal. For pressures above 50 kPa we see 1×10^{-6} repeatability, with performance degrading at lower pressures—this poorer performance is caused by the offset term in $U(p_{\mathrm{FP}})$, but uncertainty from mercury vapor in p_{UIM} is non-negligible. Notably, some bands of pressure—1 kPa, 10 kPa, and 30 kPa—are outside the expanded uncertainty of the manometer $U(p_{\mathrm{UIM}})$. At present it is not clear what to attribute these outliers to, but we are in the process of building a second laser refractometer as a cross-check, and our next tests will compare two independent laser refractometers to ultrasonic (oil and mercury) manometers.

REFERENCES

[1] P. F. Egan, J. A. Stone, J. H. Hendricks, J. E. Ricker, G. E. Scace, and G. F. Strouse, "Performance of a dual Fabry–Perot cavity refractometer," *Optics Letters*, vol. 40, no. 17, pp. 3945–3948, 2015.

[2] C. R. Tilford, "Three and a half centuries later—the modern art of liquid-column manometry," *Metrologia*, vol. 30, no. 6, pp. 545–552, 1994.

[3] J. A. Stone and A. Stejskal, "Using helium as a standard of refractive index: correcting errors in a gas refractometer," *Metrologia*, vol. 41, no. 3, pp. 189–197, 2004.

[4] H. J. Achtermann, G. Magnus, and T. K. Bose, "Refractivity virial coefficients of gaseous CH_4, C_2H_4, C_2H_6, CO_2, SF_6, H_2, N_2, He, and Ar," *The Journal of Chemical Physics*, vol. 94, no. 8, pp. 5669–5684, 1991.

[5] J. D. Dymond, K. N. Marsh, R. C. Wilhoit, and K. C. Wong, *Virial Coefficients of Pure Gases and Mixtures*, Berlin: Springer–Verlag, 2002.

[6] J. Fischer, M. de Podesta, K. Hill, M. Moldover, L. Pitre, R. Rusby, P. Steur, O. Tamura, R. White, and L. Wolber, "Present estimates of the differences between thermodynamic temperatures and the ITS-90," *International Journal of Thermophysics*, vol. 32, no. 1, pp. 12–25, 2011.

[7] P. J. Mohr, B. N. Taylor, and D. B. Newell, "CODATA recommended values of the fundamental physical constants: 2010," *Reviews of Modern Physics*, vol. 84, no. 4, pp. 1527–1605, 2012.

"Laser ReFractometer as a Transfer Standard of the Pascal."

Broadband Radiometric LED Measurements

G. P. Eppeldauer[1], C. C. Cooksey, H. W. Yoon, L. M. Hanssen,
V. B. Podobedov, R. E. Vest, U. Arp, and C. C. Miller
National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD, USA 20899

ABSTRACT

At present, broadband radiometric measurements of LEDs with uniform and low-uncertainty results are not available. Currently, either spectral radiometric measurements or broadband photometric LED measurements are used. The broadband photometric measurements are based on the CIE standardized V(λ) function, which cannot be used in the UV range and leads to large errors when blue or red LEDs are measured in its wings, where the realization is always poor. Reference irradiance meters with spectrally constant response and high-intensity LED irradiance sources were developed here to implement the previously suggested broadband radiometric LED measurement procedure [1, 2]. Using a detector with spectrally constant response, the broadband radiometric quantities of any LEDs or LED groups can be simply measured with low uncertainty without using any source standard. The spectral flatness of filtered-Si detectors and low-noise pyroelectric radiometers are compared. Examples are given for integrated irradiance measurement of UV and blue LED sources using the here introduced reference (standard) pyroelectric irradiance meters. For validation, the broadband measured integrated irradiance of several LED-365 sources were compared with the spectrally determined integrated irradiance derived from an FEL spectral irradiance lamp-standard. Integrated responsivity transfer from the reference irradiance meter to transfer standard and field UV irradiance meters is discussed.

Keywords: LED, LED radiometric measurement, broadband measurement, integrated radiometric quantities, LED integrated irradiance, UV-LED measurement, blue LED measurement, red LED measurements, flat-response LED meter, pyroelectric LED meter, filtered-Si LED meter

1. INTRODUCTION

At present, broadband UV measurements that produce uniform measurement results are not available. The International Committee on Illumination (CIE) recommends broadband UV measurements in the CIE TC2-47 Technical Report. This report is being published by the CIE Central Bureau. The report focuses on characterization of UV radiometers designed for various actinic spectra and different wavelength ranges between 200 nm and 400 nm. It also discusses calibration and measurement conditions of UV radiometers using both source- and detector-based calibration methods. Three reference-spectrum sources (Illuminant-A, blackbody, and deuterium) are proposed in the report for comparison of radiometers and also spectral mismatch corrections are applied to obtain the effective (also called broadband or integrated) responsivity. The UV radiometers discussed in the CIE report are always matched to a spectral response function, called action spectrum. The action spectrum is dimensionless (of unit 1), normalized to its maximum, and can describe an actinic effect of radiation on a radiant sensitive surface (like skin, eye, retina etc). The report also accepts action spectra like the CIE standardized UV-A, UV-B, and UV-C functions. These are all rectangular shape responsivity functions versus wavelength. Since all practical function realizations use optical filters, these rectangular-shape functions (for the UV radiometers) are usually poorly realized. The spectral mismatch errors (between the standard and realized functions) are large, resulting in significant measurement errors when the measured sources are changed (have different spectral distributions). Applying the spectral mismatch correction factors makes the measurement procedure and evaluation complicated.

Similarly, to the poor realization of the CIE standardized rectangular-shape UV responsivity-functions, the spectral mismatch errors between the realized and the CIE-standard V(λ) functions are large in the blue and red regions. In an earlier publication [3], instead of V(λ) based photometric measurements, a rectangular shape actinic function was realized

[1] george.eppeldauer@nist.gov; phone 1 301 975-2338; fax 1 301 869-5700

for the photometric wavelength range using filtered Si photodiode. The goal was to perform accurate broadband radiometric LED measurements including the blue and red intervals. Since the realized function was several percent different from the constant between the 380 nm and 780 nm wavelength limits, where the function was blocked, spectral mismatch correction was applied to decrease the measurement errors. The spectral mismatch correction factor included the spectral distribution of a standard source and the measured spectral distribution of the test-LED of a particular application. As a result of the spectral mismatch correction for the realized actinic function, the broadband radiometric LED measurements could be performed with low uncertainty for the photometric wavelength range. However, this kind of broadband measurement requires the spectral distribution measurement of the test-LED, the spectral distribution of the source used for calibration, and the relative spectral responsivity measurement of the radiometer head.

Instead of using the traditional CIE recommended source-based or detector-based calibration methods, the broadband UV measurement procedure itself can be standardized to perform simple uniform measurements with low uncertainty. The standardization of the UV measurement procedure is discussed below for broadband UV sources. In the discussed example, UV-365 sources are measured. These “black lights” are applied for fluorescent crack-recognition using liquid penetrant inspection. At present, these nondestructive tests are performed with UV-meters based on the CIE standardized UV-A function. The different spectral responsivities of the commercially available UV-meters cause large measurement errors even if the same UV-365 source is measured.

In this work, because of environmental safety reasons, the originally used Hg source (the 365 nm emission line) is substituted by a high-power LED irradiance source that peaks at around 365 nm.

In order to achieve the 1 mW/cm^2 minimum irradiance required on the test-surfaces by the American Society for Testing and Materials, ASTM-E1417 [4], high-power UV LED sources are used in the here developed irradiance sources. They produce a 7.5 cm diameter spot at a distance of 40 cm from the source. In Fig. 1, the normalized spectral power distribution (SPD) of the UV-365 LED source is compared to a monochromator measured and normalized SPD of a Hg-lamp. The Hg-lamp has a continuum radiation and the 334 nm neighboring line can be seen well in the measurement. Another advantage of the LED source is that it does not have the continuum radiation. Figure 1 also shows the spectral response curves of a few UV meters. The response curves have different peak wavelengths and different spectral widths. It can be seen that only the meters with the wider response curves around the source-peak can produce uniform (similar) measurement results. (The output signal is equal to the spectral product of the LED distribution and the spectral response of the meter). The normalized signal readings of meter (3) and meter (2) were divided by the normalized reading of meter (1) when the shown UV-365 Hg-lamp was measured. The measurement error related to meter (1) was 42 % using meter (3) and 12 % for meter (2). Standardization of the spectral response function of LED measuring radiometers cannot solve this measurement non-uniformity problem. The goal of the new standard procedure is to obtain measurement results with small errors when different meters measure LEDs (or Hg sources) with reasonable (such as +/- 5 nm) peak wavelength differences relative to the 365 nm nominal wavelength.

The standard broadband radiometric procedure discussed here as an example can be extended to LEDs or LED groups for the UV, VIS, and near-IR wavelength ranges.

2. THE UV BROADBAND MEASUREMENT PROCEDURE

In the broadband UV measurement procedure, LED source(s) is measured with a broadband meter. In the discussed example, an LED-365 irradiance source is measured by a UV irradiance meter. The measured output signal of the meter is produced by the spectral product of the source distribution and the meter response function. The requirement from the broadband measurement procedure is to obtain invariance in the measured signal (at the output of the meter) for changes in both the LED source (peak and spectral-width) and the spectral-shape of the meter-response. In order to perform uniform broadband measurements, the spectral response of the meter must be broader than the distribution of the measured source(s) and the source distribution(s) must be inside of the spectral response function of the meter for all the expected source(s) and meter changes.

The broadband measurement procedure can be applied not only for UV-365 source(s) (used in the here discussed example) but also for any other UV sources if the here described procedure-requirement(s) is achieved. In the discussed example, to obtain the invariance in the measured (output) signal, the spectral response of the meter was selected to be close to constant in a spectral range equal to or wider than the widest source-distribution of the 365-nm source to be measured. This way, the spectral product of the source-distribution(s) and meter-responsivity-function produces signals with differences (errors) less than the required measurement uncertainty when different 365-nm sources (with different peak wavelengths and spectral widths) are measured.

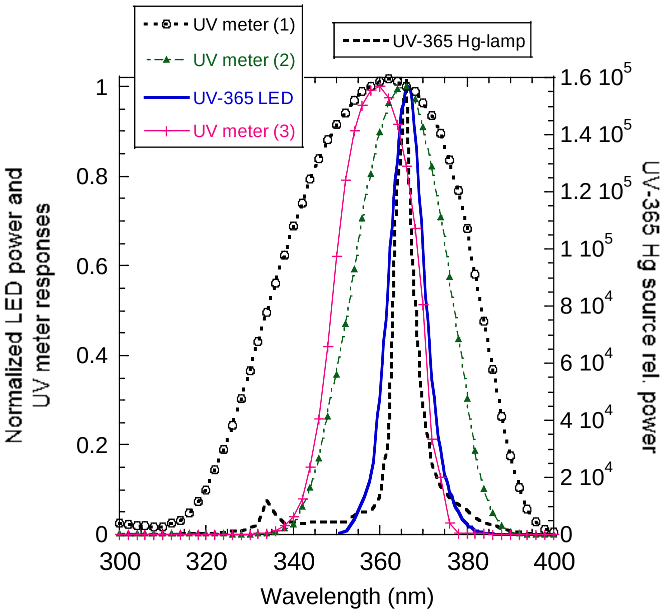


Fig. 1. Normalized distributions of Hg and LED-365 sources and UV meter responses.

Based on the here discussed procedure-requirements, existing UV meter models can be selected to obtain uniform broadband 365-nm measurements. Other UV meters, where the procedure-requirements (for spectral-responses) are not achieved, are non-ideal for uniform broadband UV measurements.

The broadband procedure can be applied for measurement of different kinds of sources, such as different single LEDs and/or a group of different LEDs, if the constant spectral response of the meter is extended to the wavelength range(s) where the measured sources emit radiation. The response deviation from constant, within the spectral range where the measured sources emit radiation, depends on the allowed uncertainty of the broadband measurement. Recently developed low-NEP pyroelectric detectors [5] are excellent candidates to measure not only UV but also other kinds of LEDs in the spectral range where the pyroelectric detector has close to constant spectral response. Based on this type of reference pyroelectric meter, the broadband scale-transfer procedure can be simplified, source standards will not be needed, and selection of the field test meters may not be needed.

3. INTEGRATED IRRADIANCE OF UV LEDS

LED-365 irradiance sources and spectrally "flat" UV irradiance meters have been developed to implement the UV broadband measurement procedure for non-destructive testing of metal parts [6]. In this application example, the excitation irradiance source peaks at a nominal wavelength of 365 nm. Typically, the purchased/applied high power LEDs have a few nm shift in their peak wavelength. In the discussed example, the peak of the purchased LED sources was at about 368 nm. Some UV irradiance meters, even if they were planned to have a constant response for the overall spectral range of the radiation produced by the LED-365 source, are spectrally "non-flat" in that range. The spectral irradiance $E(\lambda)$ of the LED-365 irradiance source and the spectral irradiance responsivity $s_{\text{ref}}(\lambda)$ of the reference UV irradiance meter (used in the discussed example), that produce the measured output signal, are shown in Fig. 2. The goal of the suggested broadband measurement procedure is to determine a responsivity for the meter that can be used to measure the integrated irradiance from a test LED source [7].

Two different versions of the calibration steps were developed depending primarily on the spectral flatness of the meter.

3.1. Non-flat response method and use of an LED-365 standard

In this first version of the broadband calibration procedure, the UV meter has a poorly realized spectrally “non-flat” response. In order to keep the procedure user-friendly and accurate, in addition to the suggested broadband calibration procedure, a standard LED-365 irradiance source was developed. The integrated irradiance from the source is measured by a reference UV irradiance meter when the separation (according to the ASTM standard) is 40 cm between source and meter. The spectral irradiance $E(\lambda)$ of the standard source is needed to determine the integrated responsivity $\bar{s}_{ref}$ of the non-flat reference UV irradiance meter. Then, the integrated irradiance responsivity can be utilized for either direct measurement of an LED-365 source(s), or it could propagate the reference-level meter-calibration to field-level calibrations or measurements.

In this version of the broadband calibration procedure [6], the following calibration steps can be used:

1) Satisfy the requirements for the spectral power distribution (SPD) of the standard source(s): Use LEDs with 365 nm ± 5 nm peaks and a maximum spectrum-half-width (FWHM) of less than 15 nm.
2) Calibrate the UV-LED excitation source for spectral irradiance (e.g. against an FEL standard lamp).
3) Select a reference irradiance meter with close to constant spectral response in the spectral interval where the measured LED emits radiation.
4) Calibrate the reference meter for spectral irradiance responsivity in the wavelength interval where the UV-LED emits radiation. Test the signal-leakage in the overall wavelength range where the detector of the meter can produce signal.
5) Calculate the output signal of the meter for the spectrally calibrated (standard) UV-LED source and a spectrally calibrated meter (using a spread-sheet).
6) Calculate the output signal of the meter by shifting the source peak ± 5 nm (to 360 nm and 370 nm) or less (depending on the uncertainty requirement for this reference scale) using the same relative spectral irradiance of the calibrated UV-LED source. The changes in the spectral product (for source and meter) are calculated to obtain the uncertainty of this reference-scale.
7) The reference UV meter can be accepted for scale transfer if the calculated output signals at the 360 nm and 370 nm wavelengths agree within the expected signal measurement uncertainty.

The above calibration steps are usually made at a national measurement institute (NMI). Utilizing steps 2 and 4, the measurement equation that describes the output signal of the reference meter for irradiance measurement mode can be written as

$$i_{ref} = \int_{\lambda} E(\lambda) s_{ref}(\lambda) \mathrm{d}\lambda \tag{1}$$

where $E(\lambda)$ is the spectral irradiance of the calibrated (standard) UV-LED source, $s_{ref}(\lambda)$ is the spectral irradiance responsivity of the reference meter, and λ is the wavelength.

Using the ASTM standardized requirement, the integrated irradiance can be determined in the reference plane of the meter, 40 cm away from the source:

$$\bar{E} = \frac{i_{ref}}{\bar{s}_{ref}} \tag{2}$$

where the integrated irradiance responsivity of the reference meter is:

$$\bar{s}_{ref} = \frac{i_{ref}}{\int E(\lambda)\mathrm{d}\lambda} \qquad (3)$$

In the discussed example, i_{ref} was both calculated (using the above mentioned spreadsheet) and measured for the LED-365 (NIST #1251) standard and the reference UV irradiance meter (NIST #130301). The calculated value of 3.13 x 10^{-5} A, was 2.2 % different from the measured value of 3.198 x 10^{-5} A. The spread-sheet calculated integrated irradiance responsivity of the reference meter was $\bar{s}_{ref}$ = 2.93 A mm^2/W. Using the measured current value, the integrated irradiance from the used LED-365 standard (NIST #1251) was 1.09 mW/cm^2, 9 % higher than the minimum irradiance level required by the ASTM standard.

After these reference-level calibration steps, the reference meter (with the known integrated responsivity) can be taken to a field laboratory where the field-level calibration steps can continue the above steps:

8) Substitute the field (test) UV meter for the reference (calibrated) UV meter in the same irradiance at the ASTM standardized 40 cm distance from the source of the standard LED-365 irradiance source and use the ratio of the meter's output signals as the calibration factor for the test UV meter. The test meter also should have close to flat spectral response in the wavelength range where the standard LED emits radiation. Otherwise, significant errors can be introduced in the measurement of the field-source during the scale transfer.

Note: Using the here discussed broadband measurement procedure, spectral response measurement of test (field) UV meters is not needed.

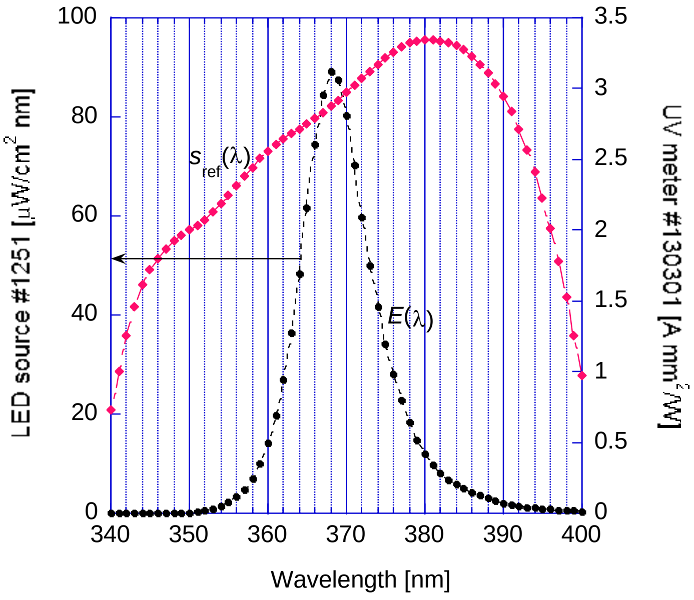


Fig 2. Spectral irradiance E(λ) of an LED-365 standard irradiance source (#1251) and spectral irradiance responsivity $s_{ref}(\lambda)$ of a reference UV irradiance meter (#130301).

3.2. UV meter-based calibrations without using a source standard

A source standard will not be needed if the reference meter has a known constant spectral responsivity for the wavelength range where the measured LED(s) emits optical radiation. Similarly, when the response of the reference meter is not constant but an average responsivity can be determined for (most of the) measured radiation, the source standard will not be needed.

3.2.1. Spectrally "flat" responsivity standard

The procedure for broadband UV calibrations and measurements can be simplified when UV meters with spectrally constant response are used. Calibration of the reference meter for constant irradiance responsivity is enough to measure the integrated irradiance (or any other output radiometric quantity) of a test LED source(s). When using these spectrally "flat" standard meters, use of a standard source is not needed. In this detector-based calibration, the only standard is the meter with the known constant spectral responsivity. When the spectral flatness (the curve shape) is known, one absolute tie point can be enough to convert the relative response function into absolute (e.g. to obtain the constant spectral irradiance responsivity).

Spectrally "flat" UV meters can be made with either filtered quantum detector (like silicon detector and glass input-filters) or pyroelectric detectors. For these "flat" meters, Eq. 1 can be applied. Since $s_{\mathrm{ref}}(\lambda) = s$ = constant, the output signal of the reference meter will be

$$i_{ref} = i = s\int_{\lambda} E(\lambda)d\lambda \qquad (4)$$

and the integrated irradiance will be

$$\overline{E} = \frac{i}{s} \qquad (5)$$

where the unit of i is A, the unit of s is A cm^2/W, and the obtained unit for $\overline{E}$ is W/cm^2.

Using a pyroelectric detector, the deviation from a spectrally constant response can be an order of magnitude smaller than using a filtered Si photodiode. Also, the wavelength coverage of a pyroelectric detector with the flat response will be much wider.

3.2.2. Average-responsivity standard

Equation 5 can also be used when the reference meter has a "non-flat" response around the peak of the measured LED. This situation is shown in Fig. 2. In this case, instead of using a spectrally constant ("flat") responsivity, the average responsivity around the LED peak can be used. In our example, the NIST #130301 reference meter was used which has a significant slope at the 368 nm peak of the measured NIST #1251 LED. Since the response-slope is symmetrical around the peak-wavelength of the measured LED within a wide enough (about +/- 8 nm) range, it was simple to determine the average responsivity for the measured LED. As can be seen in Fig. 2, the average responsivity of the meter for most of the LED radiation is 2.875 A mm^2/W, equal to the responsivity at the LED peak-wavelength. The integrated irradiance of the LED source using this "average responsivity" method will be:

$$\overline{E} = \frac{i}{s} = \frac{3125 * 10^{-8}}{2.875} = 1.087 \text{ mW/cm}^2 \qquad (6)$$

where 3125 x 10^{-8} is the sum of the measured current values between 300 nm and 400 nm calculated using a spread-sheet. The spread-sheet was made to calculate the output signal, the integrated irradiance, and the integrated responsivity for a few UV-365 sources and UV irradiance meters.

The integrated irradiance value in Eq. 6 agrees with the 1.09 mW/cm^2 obtained using $E(\lambda)$ for $\overline{s}_{ref}$ determination. This means that the two methods where the “flat” or average responsivities are used as standards, will produce equal integrated irradiance to the integrated irradiance produced by the “non-flat” meter-response method where a standard source was used (as discussed above in Section 3.1). In summary, a standard source was used for the determination of $\overline{E}$ in the non-flat response method, and no standard source is needed when the “flat” or average responsivity standards are used.

3.2.3. Use of spectrally-flat filtered-Si meters

Spectrally “flat” irradiance meters built with multilayer thin-film and glass filters were discussed earlier [6]. These meters utilized UV damage resistant nitrided Si photodiodes. These filtered meters have good stability but the curve shapes are different. The different curve-shapes are acceptable when the procedure described in Section 3.1 is used. The filtered-Si UV meters are operated in DC measurement mode. Figure 3 shows the spectral irradiance responsivity of several of these UV-365 meters. The graph also shows a monochromator measured Hg line distribution and several LED-365 source-distributions. The peak wavelengths are 3 nm or 4 nm different than the nominal 365 nm peak value. The blocking of the meters outside of the bandpass interval to about 1000 nm is at the 0.1 % level. The relative response function of six new-generation UV-365 meters is shown in Fig. 4. The maximum-to-minimum response deviation from the constant is about 3% to 10 %. Similar “flatness” is illustrated in Fig.5, where a nitrided Si photodiode was filtered to obtain a meter with close to constant response for the 345 nm to 440 nm range to measure UV and blue LEDs. The response deviation from constant is +/- 7.5 % for the realized C and +/- 7.2 % for the realized D functions.

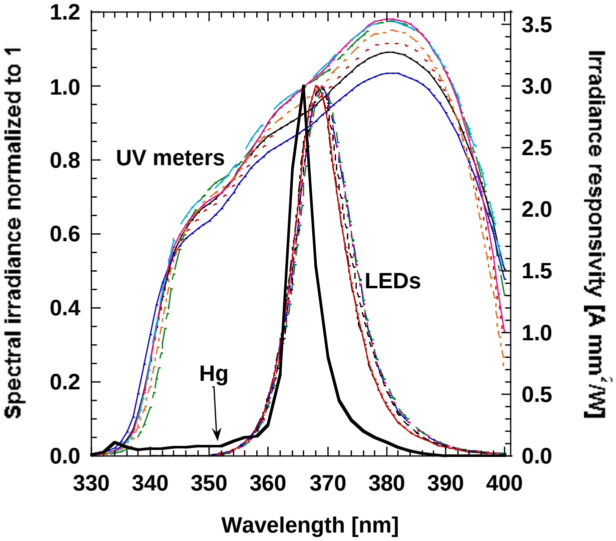


Fig. 3. Spectral irradiance of LEDs with 365 nm nominal peak, monochromator measured Hg-line distribution, and irradiance responsivity of UV-365 meters.

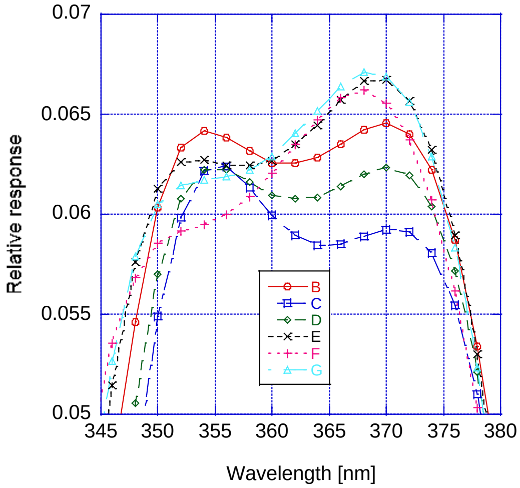


Fig. 4. Relative spectral responses of six new generation UV-365 meters (B to G).

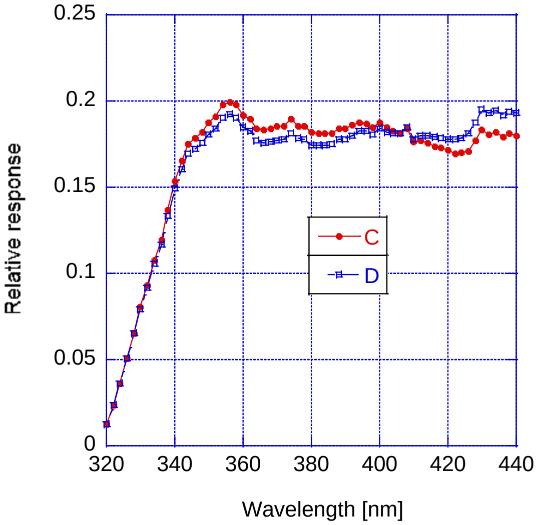


Fig. 5. Filtered Si “flat” meter for the 345 nm to 440 nm range to measure UV and blue LEDs.
Response deviation from constant is +/- 7.5 % for realization C and +/- 7.2 % for realization D.

4. ADVANCED INTEGRATED IRRADIANCE REFERENCE CALIBRATIONS

As discussed above, the integrated irradiance from LED sources can be easily measured using spectrally “flat” irradiance meters. Reference-level integrated irradiance calibrations are discussed below when using a pyroelectric “flat” irradiance meter standard.

As determined from spectral reflectance measurements, the spectral response of the reference pyroelectric detector can deviate +/- 0.1 % from constant between 330 nm and 400 nm. The deviation from constant can be a dominant uncertainty component of the integrated irradiance measured by the pyroelectric detector after its calibration. The here suggested broadband calibration will need shorter calibration time and it is less expensive than the presently applied spectral calibration techniques. Due to better spectral flatness of detector responsivity, the related measurement errors described in Section 3 can be reduced as well. As a result of the simplified broadband calibration and scale transfer, the expected combined uncertainty for the reference integrated irradiance measurement is about 0.5 % (*k*=2) which is significantly lower that the about 5 % (*k*=2) uncertainty achieved using the previously discussed methods.

The spectral irradiance responsivity calibration of a pyroelectric detector in the UV takes a few steps including the realization/transfer of absolute tie points in the visible or near-IR range, measurement of absorptance of the black coating on the top of the pyroelectric crystal, measurement of the integrated irradiance from a stable UV source and validation of this measured integrated irradiance from an independent irradiance measurement of the same UV source, in our case against an FEL lamp standard [6].

4.1. Use of spectrally flat low-NEP pyroelectric detectors

Low-NEP pyroelectric detectors available for improvement of the response deviation from constant are introduced here. Pyroelectric detectors work only in AC measurement mode therefore the output signal of the LED must be modulated. The modulation can be done either in the feeding current of the LED or with a light chopper. The modulated (AC) output signal from the meter can be measured using a simple and inexpensive lock-in amplifier.

As an example, a hybrid (detector and preamplifier are in the same metal can) pyroelectric detector that has an NEP of about 10 nW/Hz$^{1/2}$ is used here to measure five LED-365 irradiance sources. The picture of this temperature controlled detector is shown in Fig. 6. This detector can measure radiant power down to 1 μW with a signal-to-noise ratio (S/N) of 100. An organic black absorbing coating is applied on the pyroelectric detector.

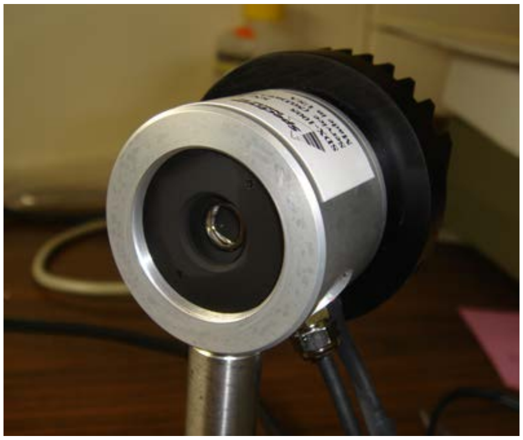


Fig. 6. Picture of a temperature controlled hybrid pyroelectric radiometer.
The $LiTaO_3$ crystal is covered with organic-black coating.

The measurements, described below, are the first time calibration of the irradiance responsivity of a pyroelectric detector. The measurements of the low-NEP pyroelectric detector were performed in AC mode using a lock-in amplifier and a chopping frequency of 10.5 Hz. A beam geometry (without using any integrating sphere) at the output of a monochromator [8] was used in the near-IR range and the irradiance responsivity scale was extended to the UV range based on the close to constant spectral absorptance (relative response) curve. For this scale extension, the output of the pyroelectric detector was compared to the output of a sphere-input extended-InGaAs (EIGA) transfer-standard for which the irradiance responsivity was known between 0.6 μm and 2.6 μm. The EIGA standard is periodically evaluated together with other NIST reference detectors to ensure that the aging effect, if any, can be neglected. In Fig. 7, the absorptance curve of the organic black coating is shown in the range of 0.25 μm to 2 μm together with a few tie points around 1 μm. The absorptance versus wavelength curve was determined from spectral reflectance measurements of the black coating. The absorptance, which is proportional to the response, is equal to 1–reflectance if the transmittance is zero. The tie points convert this relative response curve into absolute spectral irradiance responsivity. Based on the small changes in the absorptance curve, the irradiance responsivity of the pyroelectric detector was taken as a constant 910 VW^{-1}cm^{2} between 0.25 μm and 0.5 μm (in the range of the measured LED sources). However, certain variations, smaller than the measurement uncertainty, may be expected. The uncertainty of the absorptance data is a few times smaller than that of the irradiance responsivity tie points (2.6 % *k*=2), thus the uncertainty of the tie point(s) is the dominating component in the calibration uncertainty budget. It is also anticipated that the spectral irradiance responsivity follows the absorptance data obtained with the underfilled sensor area. The tie point shown at about 365 nm in Fig. 7 will be discussed in Section 4.3. The less than +/- 1 % deviations from constant up to 2 µm makes it possible to apply these broadband (integrated) irradiance LED measurements for the VIS-NIR range as well.

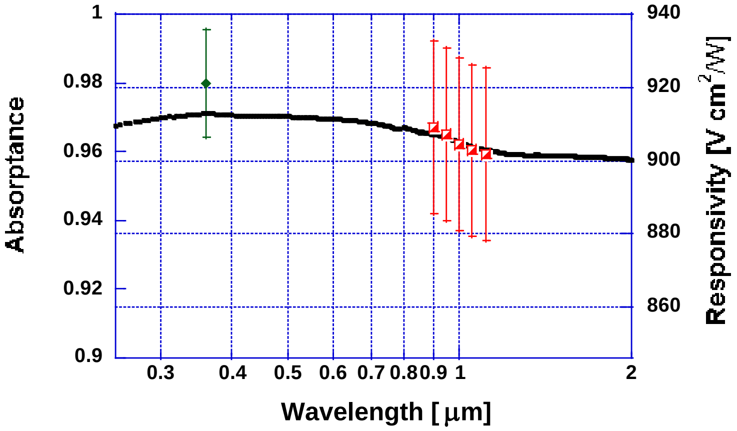


Fig. 7. Spectral absorption (1-reflectance) curve of organic black coating and irradiance responsivity tie (absolute) points derived from a sphere-input extended-InGaAs radiometer. See Section 4.3 for explanation of the tie point at 365 nm.

While the maximum deviation from the spectrally constant absorptance is +/- 0.2 % between 250 nm and 420 nm, the shown dominating 2.6 % (*k*=2) uncertainty component for the responsivity function is too high. Realizing tie points with much lower uncertainty will lead to significant improvement in the overall uncertainty of the spectral responsivity in the UV.

4.2. UV irradiance measurements using pyroelectric detector-standard and LED-365 source

The development of LED-365 irradiance source standards was discussed in our previous publications [6]. These sources were designed to satisfy the ASTM requirement to produce a target-spot irradiance of 1 mW/cm^2 or higher. This high irradiance requires 250 µW radiant power from a UV-365 source uniformly distributed on a ¼ cm^2 detector.

The irradiance from five UV sources was measured at a distance of 0.4 m. First, the irradiance non-uniformity was measured within a target-spot of 80 mm x 80 mm. The measurements were made in two orthogonal directions (along X and Y axes). The data presented in Fig. 8 indicate about 15 % irradiance non-uniformity at the distance of +/- 40 mm from the center of the output beam spot. However, in the center area of about 20 mm x 20 mm, the non-uniformity is estimated about 5 % (or about 1 % in the 5 mm x 5 mm area). It should be noted that the maximum radiation and its position with respect to the optical axis may not match and can vary from source to source. The legends (series numbers) in Fig. 9 are related to the serial numbers of the LED-365 sources. The data are normalized to the maximum radiation in the target-spot.

The irradiance produced by each LED-365 irradiance source was measured by the calibrated pyroelectric radiometer. The integrated irradiance is

$$\overline{E} = \frac{U \cdot c}{s} \qquad (7)$$

where *U* is the output voltage (in V) of the pyroelectric radiometer as measured by the lock-in amplifier, *s* is the constant spectral responsivity of the pyroelectric radiometer, equal to 910 VW^{-1}cm^2, and *c* is a conversion factor (constant) between the voltage measurements performed in AC and DC modes during the calibration. For an ideally chopped signal (with square wave shape), *c* is equal to 2.22. However, this conversion factor depends also on the actual shape of the chopped signal and it is affected by geometrical and frequency dependent factors as well. In the present measurement, *c*=2.33 was obtained using the actual geometry and calculating the ratio of the Si detector-based meter readings in DC and AC measurement modes. The summary for the integrated irradiance produced by each LED-365 source is presented in Table 1. The integrated irradiance was higher than the minimum 1 mW/cm^2 value required by the ASTM standard. The measurement uncertainty was dominated by the 2.6 % (*k*=2) uncertainty of the irradiance responsivity tie points.

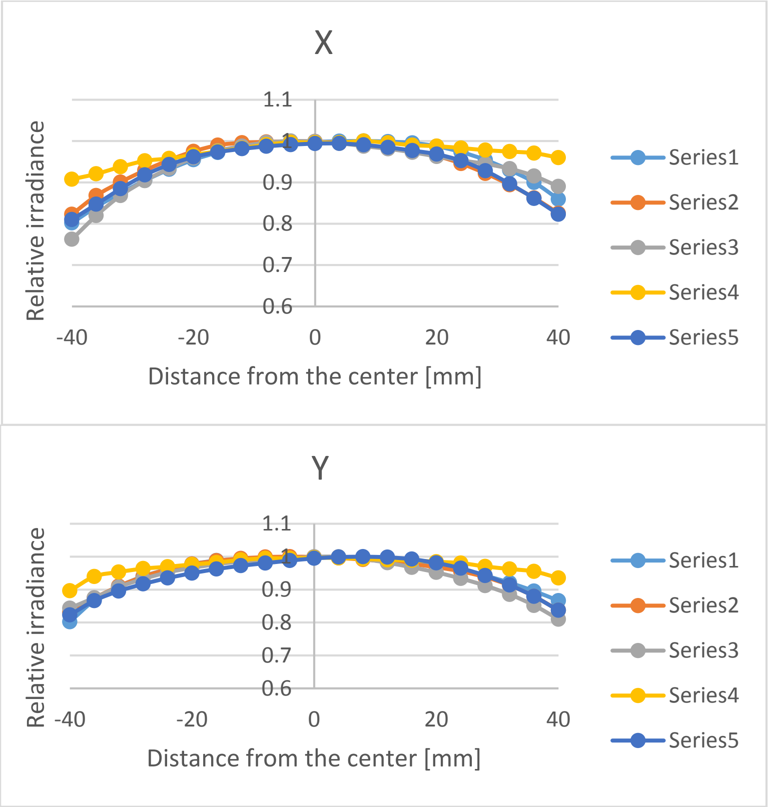


Fig. 8. Relative integrated irradiance produced by five UV irradiance sources in the 80 mm x 80 mm target-spot at a distance of 0.4 m.

Table 1. Pyroelectric radiometer output voltage and derived integrated irradiance for five LED-365 irradiance sources at a distance of 0.4 m.

Measured units / source #	**1**	**2**	**3**	**4**	**5**
U [V]	0.622	0.617	0.608	0.613	0.622
$\overline{E}$ [mW cm^{-2}]	1.59	1.58	1.56	1.57	1.59

4.3. Validation of pyroelectric detector measured integrated irradiance and UV responsivity

The integrated irradiances from five LED-365 sources of the same model were determined using two different methods. The first method, as described above, utilized the constant spectral irradiance responsivity of a low-NEP pyroelectric radiometer. In the second method, used for validation, the spectral irradiance of each LED source was derived from a traditional FEL lamp standard [6]. This spectral calibration method and setup used to determine the spectral irradiance of the UV-LED sources has already been discussed [6]. The measured spectral irradiance functions of six newly developed LED-365 irradiance sources are shown in Fig. 9. The performed spectral irradiance uncertainty was 1.6 % (*k*=2).

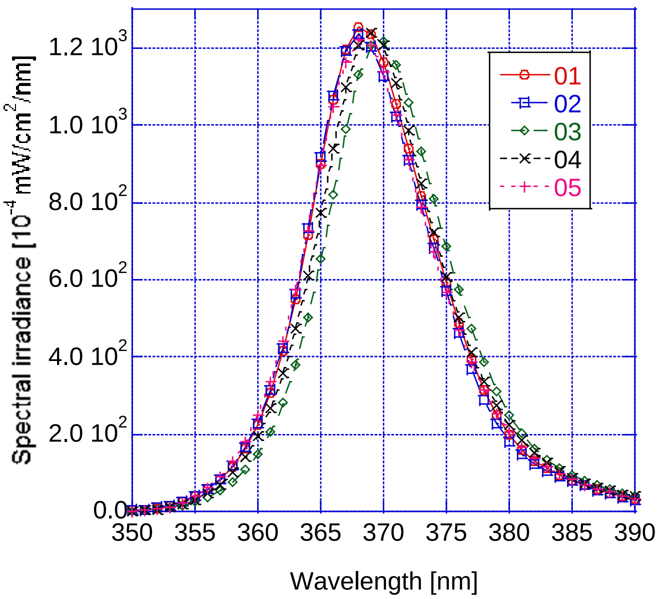


Fig. 9. Five LED-365 source standards (#01 to #05) calibrated against an FEL lamp standard.
The spectral irradiance uncertainty is 1.6 % (*k*=2).

The integrated irradiance ratios of the five LED-365 sources from the spectral and broadband measurements are shown in Table 2. The average disagreement between the integrated irradiances obtained from the two different methods is 1.2 %.

Table 2. Integrated irradiance ratios of five LED-365 sources determined from spectral and broadband calibrations.

LED#	**FEL S193 based mW/cm^2**	**Pyro-based mW/cm^2**	**FEL/Pyro**
1	1.624	1.59	**1.021**
2	1.596	1.58	**1.010**
3	1.569	1.56	**1.005**
4	1.591	1.57	**1.013**
5	1.611	1.59	**1.013**
		Average:	**1.012**

These data may be used to produce an indirect but additional tie point for calibration of irradiance responsivity of the pyroelectric detector. The tie point at 365 nm has a lower uncertainty of 1.6 % (*k*=2) versus the 2.6 % (*k*=2) found from the near-IR tie points. Thus the additional tie point presented in Fig. 7 supports the UV responsivity of the pyroelectric detector obtained from the near -IR data and absorptance in Section 4.1.

Since the maximum deviation from the spectrally constant absorptance is +/- 0.2 % between 250 nm and 420 nm, there is a possibility to significantly improve the UV responsivity scale. The future plan is to decrease the uncertainty of the irradiance responsivity tie points to the ~0.2 % (*k*=2) level using a Si-trap reference detector and also to use a high-power LED irradiance transfer source in the red. Using the high intensity LED source, the source-to-detector separation can be increased resulting in smaller distance measurement uncertainty. Applying these improvements, the planned uncertainty for the integrated irradiance measurements is less than 0.5 % (k=2).

The pyroelectric radiometer based broadband LED measurements can be applied for all kinds of LEDs or LED groups and also the measurements can be made in radiance or radiant-power modes as well.

5. INTEGRATED IRRADIANCE OF BLUE LEDS

As an example, the pyroelectric detector based broadband radiometric LED measurement was extended for deep-blue LEDs. The obtained results are presented here. LEDs with 400 nm and 405 nm peaks were selected where the responsivity deviation of the realized photopic curve is large (a few percent) compared to the CIE standard V(λ) function. One-channel surface-mount LED modules with integrated lens on a standard starboard configuration were selected. These commercially available packages were screwed to thermoelectrically controlled LED-mounts. A metal tube was attached to the LED-mount to hold a collimating convex-lens. The integrated LED-lens was located in the focus of the collimating lens of the tube. The spatial uniformity of the obtained irradiance field (as an example) is shown in Fig. 10. The separation between the source and the target was 400 mm. The diameter of the scanning aperture was 5 mm. The irradiance measurements were performed in the center-area of the target spot.

The spectral irradiance measurements, as performed with a spectrograph, for the two blue LEDs are shown in Fig. 11.

The integrated irradiance values obtained from the broadband pyroelectric-detector-based measurements are shown in Table 3. The estimated low-end limit for the pyroelectric detector measured irradiance is about 4 μW/cm^2 at a signal-to-noise ratio of 100. The 2.6 % (k=2) measurement uncertainty can be significantly improved by decreasing the uncertainty of the irradiance responsivity tie points as shown in Fig. 7.

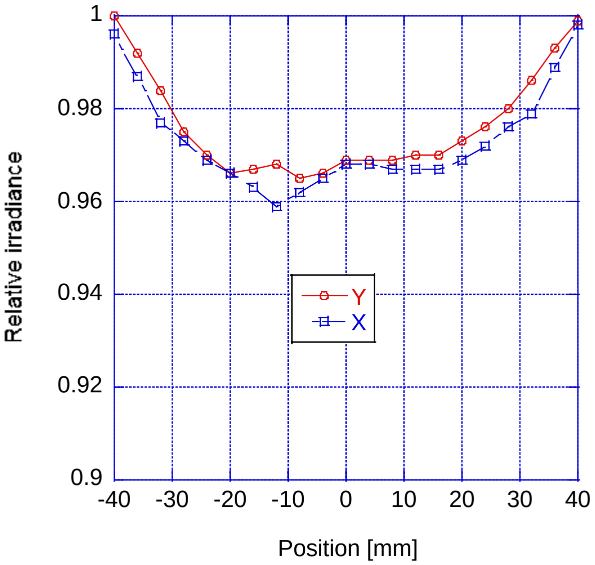


Fig. 10. Irradiance changes along the X and Y axes of the target spot from the blue (405 nm peak) LED.

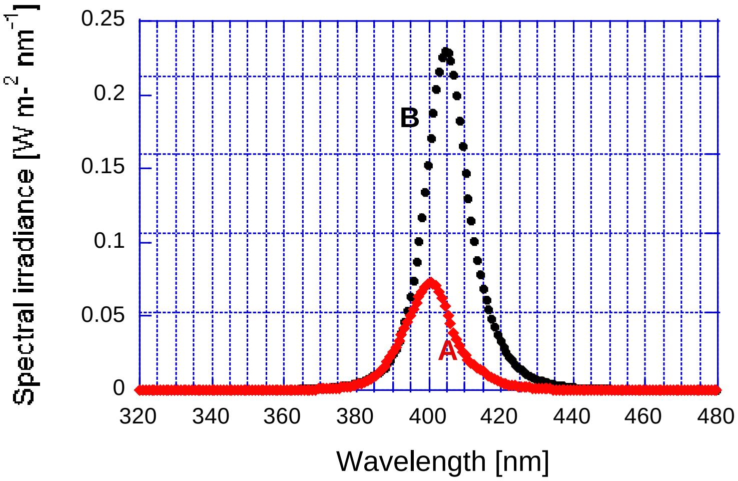


Fig. 11. Spectral irradiance measurements of two deep-blue LED sources.

Table 3. Integrated irradiance of LEDs A and B of Fig. 11.

$\overline{E}_A$ [mW/cm^2]	$\overline{E}_B$ [mW/cm^2]
0.14	0.42

6. DETERMINATION OF INTEGRATED IRRADIANCE RESPONSIVITY OF FIELD UV METERS

Utilization of the pyroelectric detector-based (standard) radiometer allows to simplify the calibration of the filtered Si transfer-standard and field UV (test) irradiance meters. The field UV meters should have a broad enough spectral response to measure the integrated irradiance from a UV source. Since these test meters are calibrated against the standard using detector-substitution when measuring the same source, the spectral flatness of these test meters is not an important issue. Before calibrating a test meter, the integrated irradiance responsivity of the pyroelectric radiometer is to be determined as described in Section 3.

In the following scale transfer, the test-meter can be substituted for the reference pyroelectric meter of known constant irradiance responsivity and the signal ratio, when they are measuring the same source, can be used to determine the "flat" irradiance responsivity of the test-meter. The integrated irradiance from the source will be equal to the ratio of the test-meter's output signal divided by the 'flat" irradiance responsivity of the test-meter. The "flat" irradiance responsivity of the test meter is

$$r_t = \mathrm{k}s \qquad (8)$$

where k is a correction factor obtained as the ratio of the test-meter output-voltage to the output-voltage of the reference meter when both measure the same irradiance. The constant irradiance responsivity of the reference (standard) meter is *s*. This responsivity, as mentioned above, is usually determined in a primary level calibration laboratory. The following simple transfer-calibrations can be performed in field calibration places. The integrated irradiance measured by the test meter will be

$$\overline{E} = \frac{U_t}{ks} \qquad (9)$$

where *U*t is the output voltage of the test irradiance meter.

Continuing our previous UV-365 source measurement examples, the integrated irradiance responsivity of any field radiometer (including existing commercial meters) may be calibrated against a calibrated filtered UV-365 (transfer standard) radiometer if the same source is used what was used earlier for the calibration of the filtered UV-365 transfer-standard irradiance meter. Also, in this case, spectral flatness for the field detector responsivity function is not required. However, if a different source is measured in the field, then the filtered UV-365 transfer-standard meter should be calibrated for that source first. If the difference between the different sources is not too high, as illustrated in the example of Fig. 9, the correction to the responsivity of the applied UV-365 transfer-standard meter could be performed using its known spectral responsivity curve (see examples of the functions in Figs. 3 to 5).

7. CONCLUSIONS

A broadband radiometric measurement procedure has been developed to perform uniform LED calibrations and measurements with low uncertainty. As an example, the procedure has been implemented here for UV and blue LEDs. For reference-level calibrations, LED-365 irradiance source standards and UV irradiance meters have been developed. Using a low-NEP pyroelectric radiometer, a UV response function with +/- 0.2 % maximum deviation from constant has been realized between 250 nm and 420 nm. Using the constant irradiance responsivity of a reference pyroelectric radiometer, the integrated irradiance from all kinds of LEDs can be measured without using a source standard. The 2.6 % (k=2) uncertainty, dominated by the irradiance responsivity reference (absolute tie) points for the pyroelectric radiometer, can be improved significantly. The developed LED-365 irradiance sources and UV irradiance meters can be used to calibrate field UV irradiance meters against the working standard meter when using the same LED-365 source. Using the pyroelectric standard based broadband procedure, yearly spectral calibrations for the working standards is not needed. Also, any field radiometer (including existing commercial meters) may be calibrated against a calibrated (filtered) UV-365 (transfer standard) radiometer if the same source is used what was used earlier for the calibration of the filtered UV-365 transfer-standard meter. In this case, spectral flatness for the field detector responsivity function is not required. When a different source is measured in the field, then the filtered UV-365 transfer-standard meter should be calibrated for that source first. If the difference between the different sources is not too high (as illustrated in the example of Fig. 9), the correction to the responsivity of the applied UV-365 transfer-standard meter could be performed using its known spectral responsivity curve. Using the discussed broadband calibration procedure, fast, inexpensive, and accurate LED measurements can be performed in irradiance, radiance, or radiant-power modes.

References

1. Eppeldauer, G.P., *Standardization of broad-band UV measurements for 365 nm LED sources.* J. Res. Natl. Inst. Standards and Technology, 2012. **117**: p. 96-103.
2. Eppeldauer, G.P., *Standardization of broadband UV measurements.* UVNews 9, Newsletter of the Thematic Network for Ultraviolet Measurements of the European Metrology Research Program of EURAMET, 2013. **Published by Aalto University, Helsinki, Finland.**(9/January): p. 34-37.
3. Gugg-Helminger, A., et al., *Broadband radiometric measurement of LED devices.* CIE Conference, Leon, Spain, 2005.
4. ASTM-E1417, *Liquid Penetrant Examination Standard.*
5. Eppeldauer, G.P., J. Zeng, and H.W. Yoon, *Low NEP pyroelectric radiometer standards.* SPIE Proc., 2008. **6940**: p. 694036-1 to 694036-8.
6. Eppeldauer, G.P., T.C. Larason, and H.W. Yoon, *Standardization of UV LED measurements.* Proc. SPIE, 2015. **9571**(14th International Conf. on Solid State Lighting and LED-based Illumination Systems): p. 957105-1 to 957105-12.
7. Eppeldauer, G.P., et al., *Calibration procedure for UV-365 integrated irradiance measurements.* CIE 28th Session Proc., 2015. **Manchester, GB**.
8. Podobedov, V.B., et al., *Calibration of spectral responsivity of IR detectors in the range from 0.6 mm to 24 mm.* SPIE Proceedings, 2016. **9819** (Infrared Technology and Applications XLII, 98190P (May 20, 2016); doi:10.1117/12.2228384).

Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)

David Ferraiolo, Ramaswamy Chandramouli, Rick Kuhn and Vincent Hu

National Institute of Standards and Technology
Gaithersburg, Maryland 20899
{dferraiolo, mouli, Kuhn, vhu}@nist.gov

ABSTRACT

Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC) are very different attribute based access control standards with similar goals and objectives. An objective of both is to provide a standardized way for expressing and enforcing vastly diverse access control policies in support of various types of data services. The two standards differ with respect to the manner in which access control policies and attributes are specified and managed, and decisions are computed and enforced. This paper is presented as a consolidation and refinement of public draft NIST SP 800-178 [21], describing, and comparing these two standards.

Keywords

ABAC; XACML; NGAC; Policy Machine; Access Control

1. INTRODUCTION

Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC) offer different approaches to attribute based access control (ABAC). XACML, available since 2003, is an Extensible Markup Language (XML) based language standard designed to express security policies, as well as the access requests and responses needed for querying the policy system and reaching an authorization decision [17]. XACML was developed as collaboration among vendors with a goal to separate policy expression and decision-making from proprietary operating environments in support of the access control needs of applications. NGAC is an emerging, relations and architecture-based standard designed to express and enforce access control policies, through configuration of relations [2], [20]. NGAC stems from and is in alignment with the Policy Machine, a research effort to develop a general-purpose ABAC framework [6], [7], [8], [9].

What are the similarities and differences between these two standards? What are their comparative advantages and disadvantages? These questions are particularly relevant because XACML and NGAC provide different means of achieving a common access control goal—to allow vastly different access policies to be expressed and enforced in data services using the features of the same underlying mechanism in diverse ways. These are also important questions, given the prevalence of data services in computing. Data services include computational capabilities that allow the consumption, alteration, management, and sharing of data resources. Data services can take on many forms, to include applications such as time and attendance reporting, payroll processing, and health benefits management, but also including system level utilities such as file management.

This paper describes XACML and NGAC and compares them with respect to five criteria. The first criterion is the relative degree to which the access control logic of a data service can be separated from a proprietary operational environment. The other four criteria are derived from ABAC issues or considerations identified by NIST Special Publication (SP) 800-162 [13]: operational efficiency, attribute and policy management, scope and type of policy support, and support for administrative review and resource discovery.

2. BACKGROUND

Controlling and managing access to sensitive data has been an ongoing challenge for decades. ABAC represents the latest milestone in the evolution of logical access control methods. It provides an attribute-based approach to accommodate a wide breadth of access control policies and simplify access control management.

Most other access control approaches are based on the identity of a user requesting execution of a capability to perform an operation on a data resource (e.g., read a file), either directly via the user's identity, or indirectly through predefined attribute types such as roles or groups assigned to the user. Practitioners have noted that these forms of access control are often cumbersome to set up and manage, given their need to, and the difficulty of, associating capabilities directly to users or their attributes. Furthermore, the identity, group, and role qualifiers of a requesting user are often insufficient for expressing real-world access control policies. An alternative is to grant or deny user requests based on arbitrary attributes of users and arbitrary attributes of data resources, and optionally environmental attributes that may be globally recognized and tailored to the policies at hand. This approach to access control is commonly referred to as attribute-based access control (ABAC) and is an inherent feature of both XACML and NGAC.

The XACML and NGAC standards also enable decoupling of data service access control logic from proprietary operating environments (e.g., operating system, middleware, application).

This paper is authored by an employee(s) of the United States Government and is in the public domain. Non-exclusive copying or redistribution is allowed, provided that the article citation is given and the authors and agency are clearly identified as its source.

ABAC'16, March 11 2016, New Orleans, LA, USA
ACM 978-1-4503-4079-3/16/03
DOI: http://dx.doi.org/10.1145/2875491.2875496

Ferraiolo, David; Chandramouli, Ramaswamy; Kuhn, David; Hu, Chung Tong.
"Extensible Access Control Markup Language (XACML) and
Next Generation Access Control (NGAC)." Paper presented at the
ABAC'16: 2016 ACM International Workshop on Attribute Based
Access Control, New Orleans, LA, Mar 11-Mar 11, 2016.

More precisely, a data service is normally comprised of an application layer and an operating environment layer that can be delineated by their functionality and interfaces. The application layer provides a user interface and methods for presentation, manipulation, management and sharing of data. The application layer does not carry out operations that consume data, alter the state of data, organize data, or alter the access state to data, but instead issue requests to the operating environment layer to perform those operations. An operating environment implements operational routines (e.g., read, write/save) to carry out application access requests as well as access control routines to ensure executions of user processes involving operational routines are policy preserving.

Access control routines comprise several components that work together to bring about policy-preserving data resource access. These components include access control data for expressing access control policies and representing attributes, and a set of functions for trapping access requests, and computing and enforcing access decisions over those requests. Most operating environments implement access control in different ways, each with a different scope of control (e.g., users, resources), and each with respect to different operation types (e.g., read, send, approve, select) and data resource types (e.g., files, messages, work items, records).

This heterogeneity introduces a number of administrative and policy enforcement challenges. Administrators are forced to contend with a multitude of security domains when managing access policies and attributes. Even if properly coordinated across operating environments, global controls are hard to visualize and implement in a piecemeal fashion. Furthermore, because operating environments implement access control in different ways, it is difficult to exchange and share access control information across operating environments. XACML and NGAC seek to alleviate these problems by creating a common and centralized way of expressing all access control data (policies and attributes) and computing and enforcing decisions, over the access requests from applications.

3. XACML

For purposes of brevity and readability, the XACML specification is presented as a summary that is intended to highlight XACML's salient features and should not be considered complete. In some instances, actual XACML terms are substituted with equivalent terms to accommodate a simpler and more consolidated presentation.

3.1 Attributes and Policies

An XACML access request consists of subject attributes (typically for the user who issued the request), resource attributes (the resource for which access is sought), action attributes (the operations to be performed on the resource), and environment attributes.

XACML attributes are specified as name-value pairs, where attribute values can be of different types (e.g., integer, string). An attribute name/ID denotes the property or characteristic associated with a subject, resource, action, or environment. For example, in a medical setting, the attribute name Role associated with a subject may have doctor, intern, and admissions nurse values, all of type string. Subject and resource instances are specified using a set of name-value pairs for their respective attributes. For example, the subject attributes used in a Medical Policy may include: Role = "doctor", Ward = "pediatrics"; an environmental attribute: Time = 12:11; and resource attributes: Resource-id = "medical-records", WardLocation = "pediatrics", Patient = "johnson".

Subject and resource attributes are stored in repositories and are retrieved through the Policy Information Point (PIP) at the time of an access request and prior to or during the computation of the decision. XACML formally defines an action as a component of a request with attribute values that specify operations such as read, write, submit, and approve.

Environmental attributes, which depend on the availability of system sensors that can detect and report values, are somewhat different from subject and resource attributes, which are administratively created. These environmental characteristics are subject and resource independent, and may include the current time, day of the week, or threat level.

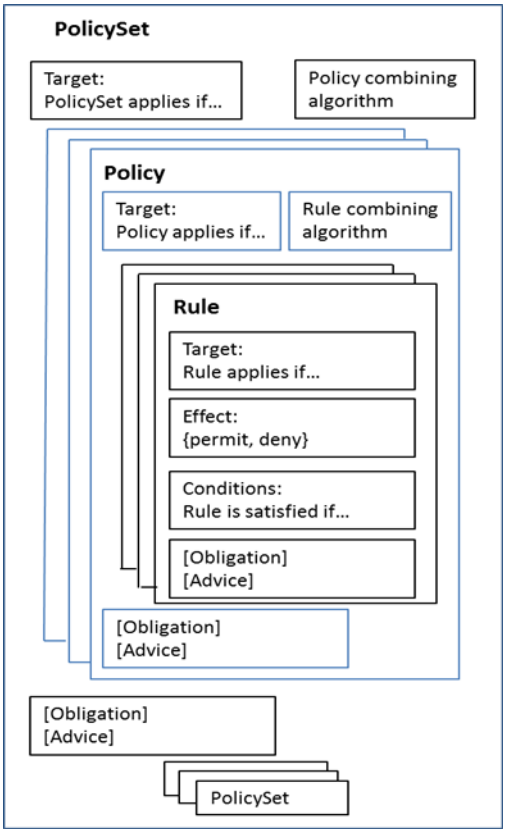


Figure 1. XACML Policy Constructs

As shown by Figure 1, XACML access policies are structured as PolicySets that are composed of Policies and optionally other PolicySets, and Policies that are composed of Rules. Policies and PolicySets are stored in a Policy Retrieval Point (PRP). Because not all Rules, Policies, or PolicySets are relevant to a given request, XACML includes the notion of a Target. A Target defines a simple Boolean condition that, if satisfied (evaluates to True) by the attributes, establishes the need for subsequent evaluation by a Policy Decision Point (PDP). If no Target matches the request, the decision computed by the PDP is NotApplicable.

In addition to a Target, a rule includes a series of boolean conditions that if evaluated True have an effect of either Permit or Deny. If the target condition evaluates to True for a Rule and the Rule's condition fails to evaluate for any reason, the effect of the Rule is Indeterminate. In comparison to the (matching) condition of a Target, the conditions of a Rule or Policy are typically more complex and may include functions (e.g., “greater-than-equal”, “less-than”, “string-equal”) for the comparison of attribute values. Conditions can be used to express access control relations (e.g., a doctor can only view a medical record of a patient assigned to the doctor’s ward) or computations on attribute values (e.g., sum(x, y) less-than-equal:250).

3.2 Combining Algorithms

Because a Policy may contain multiple Rules, and a PolicySet may contain multiple Policies or PolicySets, each Rule, Policy, or PolicySet may evaluate to different decisions (Permit, Deny, NotApplicable, or Indeterminate). XACML provides a way of reconciling the decisions each makes. This reconciliation is achieved through a collection of combining algorithms. Each algorithm represents a different way of combining multiple local decisions into a single global decision. There are several combining algorithms, to include the following:

- Deny-overrides: if any decision evaluates to Deny, or no decision evaluates to Permit, then the result is Deny. If all decisions evaluate to Permit, the result is Permit.
- Permit-overrides: if any decision evaluates to Permit, then the result is Permit, otherwise the result is Deny.

Combining algorithms are applied to rules in a Policy and Policies within a PolicySet in arriving at an ultimate decision of the PDP. Combining algorithms can be used to build up increasingly complex policies. For example, given that a subject request is Permitted (by the PDP) only if the aggregate (ultimate) decision is Permit, the effect of the Permit-overrides combining algorithm is an “OR” operation on Permit (any decision can evaluate to Permit), and the effect of a Deny-overrides is an “AND” operation on Permit (all decisions must evaluate to Permit).

3.3 Obligations and Advice

XACML includes the concepts of obligation and advice expressions. An obligation optionally specified in a Rule, Policy, or PolicySet is a directive from the PDP to the Policy Enforcement Point (PEP) on what must be carried out before or after an access request is approved or denied. Advice is similar to an obligation, except that advice may be ignored by the PEP. A few examples include:

- If Alice is denied access to document X: email her manager that Alice tried to access document X.
- If a user is denied access to a file: inform the user why the access was denied.
- If a user is approved to view document X: watermark the document “DRAFT” before delivery.

3.4 Example Policy

Consider the following example XACML policy specification. For purposes of maintaining the same semantics as XACML, we use the same element names, but specify policies and rules in pseudocode for purposes of enhanced readability (instead of exact XACML syntax).

Policy 1 applies to “All read or write accesses to medical records by a doctor or intern” (the target of the policy) and includes three rules. As such, the policy is considered “applicable” whenever a subject with a role of “doctor” or “intern” issues a request to read or write a “medical-records” resource. The rules do not refine the target, but describe the conditions under which read or write requests from doctors or interns to medical records can be allowed. Rule 1 will deny any access request (read or write) if the ward in which the doctor or intern is assigned is not the same ward where the patient is located. Rule 2 explicitly denies “write” access requests to interns under all conditions. Rule 3 permits read or write access to medical-records for “doctor”, regardless of Rule 1, if an additional condition is met. This additional condition pertains to patients in critical status. Since the intent of the policy is to allow access under these critical situations, a policy combining algorithm of “permit-overrides” is used, while still denying access if only the conditions stated in Rule 1 or Rule 2 apply.

```
<Policy PolicyId = “Policy 1” rule-combining-algorithm=”permit-overrides”>
        // Doctor Access to Medical Records //
   <Target>
     /* :Attribute-Category    :Attribute ID    :Attribute Value */
           :access-subject     :Role            :doctor
           :access-subject     :Role            :intern
           :resource           :Resource-id     :medical-records
           :action             :Action-id       :read
           :action             :Action-id       :write
    </Target>

    <Rule RuleId = “Rule 1” Effect=”Deny”>
         <Condition>
   Function: string-not-equal
           /* :Attribute-Category   :Attribute ID */
                :access-subject      :WardAssignment
                :resource            :WardLocation
         </Condition>
     </Rule>

     <Rule RuleId = “Rule 2” Effect=”Deny”>
         <Condition>
   Function: string-equal
        /* :Attribute-Category   :Attribute ID   :Attribute Value */
                :access-subject      :Role            :intern
                :action              :Action-id       :write
          </Condition>
     </Rule>

     <Rule RuleId = “Rule 3” Effect=”Permit”>
         <Condition>
  Function:and
    Function: string-equal
        /* :Attribute-Category   Attribute ID    :Attribute Value */
                :access-subject      :Role            :doctor
   Function: string-equal
         /* :Attribute-Category   :Attribute ID   :Attribute Value */
                :resource            :PatientStatus    :critical
         </Condition>
     </Rule>
 </Policy>
```

Together policies (PolicySets and Policies) and attribute assignments define the authorization state. Table 1 defines the authorization state for Policy 1 by specifying attribute names and values. We use a functional notation for reporting on attribute values with the format A(), where the parameter may be a subject or resource.

Table 1. Attribute Names and Values and the Authorization

State for Policy 1

Subject Attribute Names and their Domains:
Role = {doctor, intern}
WardAssignment = {ward1, ward2}

Resource Attribute Names and their Domains:
Resource-id = {medical-records}
WardLocation = {ward1, ward2}
PatientStatus = {critical}

Action Attribute Names and their Domains: Action-id = {read (r), write (w)}
Attribute value assignments when there are two subjects (s1, s2) and three resources (r1, r2, r3): A(s1) = <doctor, ward2>, A(s2) = <intern, ward1>, A(r1) = <medical-records, ward2, ‘ ‘>, A(r2) = <medical-records, ward1, ‘ ‘>, and A(r3) = < medical-records, ward1, critical>.
Authorization state: (s1, r, r1), (s1, w, r1), (s1, r, r3), (s1, w, r3), (s2, r, r2)

3.5 Delegation

The XACML Policies discussed thus far have pertained to Access Policies that are created and may be modified by an authorized administrator. These access policies are not associated with a specific “Issuer” and are considered “trusted”. As such, a “Trusted Access Policy” is directly used by the PDP in a combining algorithm applicable for the policy. In situations where policy creation needs to be delegated from a centralized administrator to a subordinate administrator, there is the need to create a new category of policies that control what policies can be created by the subordinate administrators. This new category of policies is called “Administrative Policies”. Similer to Access Policies, Administrative Policies not associated with a specific issuer are considered trusted and refered to as “Trusted Administrative Policies”.

Administrative policies include a delegate and a situation in its Target. A *situation* scopes the access rights that can be delegated and may include some combination of subject, resource, and action attributes. The *delegate* is an attribute category of the same type as a subject, representing the entity(s) that has (have) been given the authority to create either access or further delegation rights. If the delegate creates an Access Policy, then he/she becomes the “Issuer” for that policy. Such an Access Policy then is considered an “Untrusted Access Policy” since the authority under which it was created has to be verified. Similarly, when the delegate creates an “Administrative Policy”, the newly created policy is considered as an “Untrusted Administrative Policy” with the same trust verification requirement as “Untrusted Access Policy”.

Trusted Administrative Policies serve as a root of trust. They are created under the same authority used to create trusted Access Policies. A Trusted Administrative Policy gives the delegate the authority to create Untrusted Administrative Policies or Untrusted Access Policies. The *situation* for a newly created Untrusted Administrative Policy or Untrusted Access Policy is a subset (the same or narrower in scope) of that specified in the Trusted Administrative Policy. In addition, an Untrusted Administrative Policy or Untrusted Access Policy includes a *policy issuer* tag with a value that is the same as that of the delegate in the Administrative Policy under which it was created. Both of these policies have at least one rule with a PERMIT or DENY effect.

XACML with delegation profile recognizes two types of requests – Access Requests and Administrative Requests. Access Requests are issued to (attempt to match targets of) Access Policies or Untrusted Access Policies. An Untrusted Access Policy includes a Policy Issuer tag and an Access Policy does not. If the Access Request matches the target of an Access Policy, the PDP considers the Access Policy authorized and it is directly used by the PDP in a combining algorithm to arrive at a final access decision. If the Access Request matches the target of an Untrusted Access Policy, the authority of the policy issuer must first be verified before it can be considered by the PDP. Authority is determined through establishment of a *delegation chain* from the Untrusted Access Policy, through potentially zero or more Untrusted Administrative Policies, to a Trusted Administrative Policy. If the authority of the policy issuer can be verified, the PDP evaluates the access request against the Untrusted Access Policy; otherwise it is considered an unauthorized policy and discarded. In a graph where policies are nodes, a delegation chain consists of a series of edges from the node representing an Untrusted Access Policy to a Trusted Administrative Policy. To construct each edge of the graph, the XACML context handler formulates Administrative Requests.

An Administrative Request has the same structure as an Access Request except that in addition to attribute categories – access-subject, resource, and action – it also uses two additional attribute categories, delegate and decision-info. If a policy Px happens to be one of the applicable (matched) Untrusted Access Policies, the administrative request is generated using policy Px to construct an edge to policy Py using the following:

- Convert all Attributes (and attribute values) used in the original Access Request to attributes of category delegated.
- Include the value under the *PolicyIssuer* tag of Px as value for the subject-id attribute of the *delegate* attribute category.
- Include the effect of evaluating policy Px as attribute value (PERMIT, DENY, etc.) for the Decision attribute of *decision-info* attribute category.

The Administrative Request constructed is evaluated against the target for a policy Py. If the result of the evaluation is “Permit”, an edge is constructed between policies Px and Py. The objective is to verify the authority for issuance of policy Px. For this to occur there must exist a policy with its “delegate” set to the policy issuer of Px. If that policy is Py, then it means policy Px has been issued under the authority found in policy Py. The edge construction then proceeds from policy Py until an edge to a Trusted Administrative Policy is found. The process of selecting applicable policies for inclusion in the combining algorithm is illustrated in Figure 2.

By matching of the attributes in the original access request to the targets in various policies, Untrusted Access Policies P31, P32, and P33 can be found applicable. A path to a Trusted Administrative Policy P11 can be found directly from the applicable Untrusted Access Policy P31. A path to a Trusted Administrative Policy P12 can be found through Untrusted Administrative Policy P22 for the applicable Untrusted Access Policy P32. Because no such path can be found for P33, only the policies P31 and P32 will be used in the combining algorithm for evaluating the final access decision.

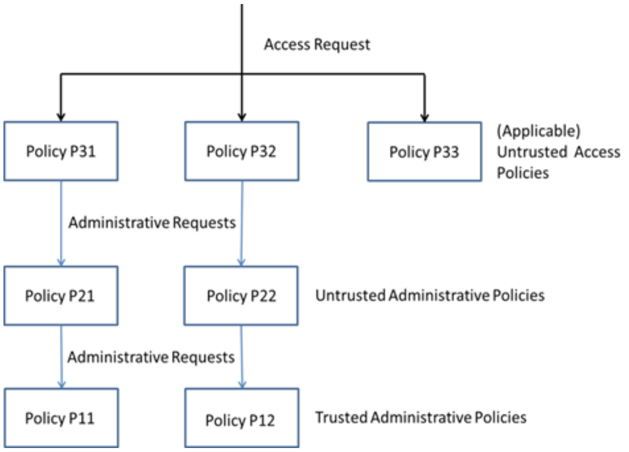


Figure 2. Utilizing Delegation Chains for Policy Evaluation

3.6 Reference Architecture

XACML reference architecture defines necessary functional components (depicted in figure 3) to achieve enforcement of its policies. The authorization process depends on four layers of functionality: Enforcement, Decision, Access Control Data, and Administration.

At its core is a PDP that computes decisions to permit or deny subject requests (to perform actions on resources). Requests are issued from, and PDP decisions are returned to a PEP using a request and response language. To convert access requests in native format (of the operating environment) to XACML access requests (or convert a PDP response in XACML to a native format), the XACML architecture includes a context handler. In the reference architecture in Figure 3, the context handler is not explicitly shown as a component since we assume that it is an integral part of the PEP or PDP.

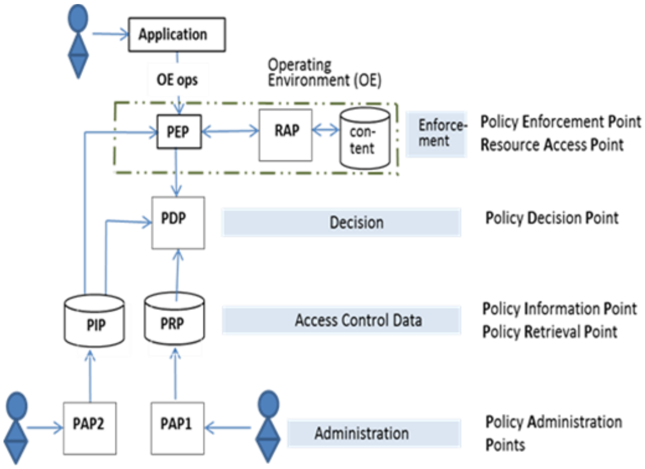


Figure 3. XACML Reference Architecture

A request is comprised of attributes extracted from the PIP, minimally sufficient for Target matching. The PIP is shown as one logical store, but in fact may comprise multiple physical stores. In computing a decision, the PDP queries policies stored in a PRP. If the attributes of the request are not sufficient for rule and policy evaluation, the PDP may request the context handler to search the PIP for additional attributes. Information and data stored in the PIP and PRP comprise the access control data and collectively define the current authorization state.

A Policy Administration Point (PAP1) using the XACML policy language creates the access control data stored in the PRP in terms of rules for specifying Policies, PolicySets as a container of Policies, and rule and combining algorithms. The PRP may store trusted or untrusted policies. Although not included in the XACML reference architecture, we show a second Policy Administration Point (PAP2) for creating and managing the access control data stored in the PIP. PAP2 implements administrative routines necessary for the creation and management of attribute names and values for users and resources. The Resource Access Point (RAP) implements routines for performing operations on a resource that is appropriate for the resource type. In the event that the PDP returns a permit decision, the PEP issues a command to the RAP for execution of the approved operation resource pair. As indicated by the dashed box in Figure 3, the RAP, in addition to the PEP, runs in an application's operating environment, independent of the PDP and its supporting components. The PDP and its supporting components are typically implemented as modules of a centralized Authorization Server that provides authorization services for arbitrary types of operations.

4. NGAC

NGAC takes a fundamentally different approach from XACML for representing requests, expressing and administering policies, representing and administering attributes, and computing and enforcing decisions. NGAC is defined in terms of a standardized and generic set of relations and functions that are reusable in the expression and enforcement of policies.

For purposes of brevity and readability, the NGAC specification is presented as a summary that highlights NGAC's salient features and should not be considered complete. In some instances, actual NGAC relational details and terms are substituted with others to accommodate a simpler presentation.

4.1 Policy and Attribute Elements

NGAC's access control data is comprised of basic elements, containers, and configurable relations. While XACML uses the terms subject, action, and resource, NGAC uses the terms user, operation, and object with similar meanings. In addition to these, NGAC includes processes, administrative operations, and policy classes. Like XACML, NGAC recognizes user and object attributes; however, it treats attributes along with policy class entities as containers. These containers are instrumental in both formulating and administering policies and attributes. NGAC treats users and processes as independent but related entities. Processes through which a user attempts access take on the same attributes as the invoking user.

Although an XACML resource is similar to an NGAC object, NGAC uses the term object as an indirect reference to its data content. Every object is an object attribute. The reference to an object is the value of its "name" attribute. Thus the value of the "name" attribute of an object is synonimus with the object. The set of objects reflects entities needing protection, such as files, clipboards, email messages, and record fields.

Similar to an XACML subject attribute value, NGAC user containers can represent roles, affiliations, or other common characteristics pertinent to policy, such as security clearances.

Object containers (attributes) characterize data and other resources by identifying collections of objects, such as those associated with certain projects, applications, or security classifications. Object containers can also represent compound objects, such as folders, inboxes, table columns, or rows, to satisfy the requirements of different data services. Policy class containers are used to group and characterize collections of policy or data services at a broad level, with each container representing a distinct set of related policy elements. Every user, user attribute, and object attribute must be contained in at least one policy class. Policy classes can be mutually exclusive or overlap to various degrees to meet a range of policy requirements.

NGAC recognizes a generic set of operations that include basic input and output operations (i.e., read and write) that can be performed on the contents of objects that represent data service resources, and a standard set of administrative operations that can be performed on NGAC access control data that represent policies and attributes. In addition, an NGAC deployment may consider and provide control over other types of resource operations besides the basic input/output operations. Administrative operations, on the other hand, pertain only to the creation and deletion of NGAC data elements and relations, and are a stable part of the NGAC framework.

4.2 Relations

NGAC does not express policies through rules, but instead through configurations of relations of four types: assignments (define membership in containers), associations (to derive privileges), prohibitions (to derive privilege exceptions), and obligations (to dynamically alter access state).

4.2.1 Assignments and Associations

NGAC uses a tuple (x, y) to specify the assignment of element x to element y. In this publication we use the notation x→y to denote the same assignment relation. The assignment relation always implies containment (x is contained in y). The set of entities used in assignments include users, user attributes, and object attributes (which include all objects), and policy classes.

To be able to carry out an operation, one or more access rights are required. As with operations, two types of access rights apply: non-administrative and administrative.

Access rights to perform operations are acquired through associations. An association is a triple, denoted by *ua*---*ars*---*at*, where *ua* is a user attribute, *ars* is a set of access rights, and *at* is an attribute, where *at* may comprise either a user attribute or an object attribute. The attribute *at* in an association is used as a referent for itself and the policy elements contained by the attribute. Similarly, the first term of the association, attribute *ua*, is treated as a referent for the users contained in *ua*. The meaning of the association *ua*---*ars*---*at* is that the users contained in *ua* can execute the access rights in *ars* on the policy elements referenced by *at*. The set of policy elements referenced by *at* is dependent on (and meaningful to) the access rights in *ars*.

Figure 4 illustrates assignment and association relations depicted as a graphs with two policy classes—Project Access, and File Management. Users and user attributes are on the left side of the graphs, and objects and object attributes are on the right. The arrows represent assignment or containment relations and the dashed lines denote associations.

Collectively associations and assignments indirectly specify privileges of the form (*u*, *ar*, *e*), with the meaning that user *u* is permitted (or has a capability) to execute the access right *ar* on element *e*, where *e* can represent a user, user attribute, or object attribute. Determining the existence of a privilege (a derived relation) is a requirement of, but as we discuss later, not sufficient in computing an access decision.

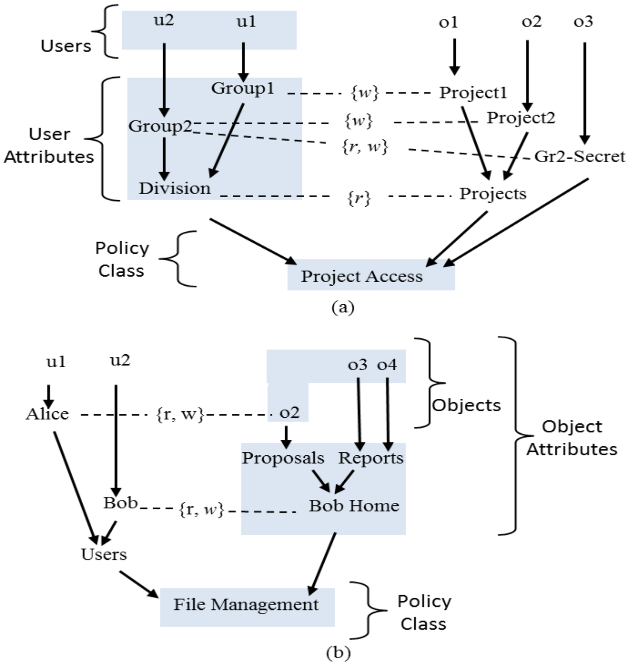


Figure 4: Two Example Assignment and Association Graphs

NGAC includes an algorithm for determining privileges with respect to one or more policy classes and associations. Specifically, (*u*, *ar*, *e*) is a privilege, if and only if, for each policy class *pc* in which *e* is contained, the following is true:

- The user *u* is contained by the user attribute of an association;
- The element *e* is contained by the attribute *at* of that association;
- The attribute *at* of that association is contained by the policy class *pc*, and
- The access right *ar* is a member of the access right set of that association.

The left and right columns of Table 2 respectively list derived privileges for Figures 4a and 4b, when considered independent of one another. Table 3 lists the privileges for these graphs in combination.

Note that (*u*1 *r*, *o*1) is a privilege in table 3 because o1 is only in policy class Project Access and there exist an association Division---{*r*}--- Projects, where u1 is in Division, r is in {r}, and o1 is in Projects. Note that (*u*1, *w*, *o*2) is not a privilege in table 3 because o2 is in both Project Access and File Management policy classes, and although there exist an association Alice---{r, w}---o2, where u1 is in Alice, w is in {r, w}, and o2 is in o2 and File Management, no such association exists with respect to Project Access.

Table 2: List of derived privileges for the independent configuration of Figures 4a and 4b

(*u*1, *r*, *o*1), (*u*1, *w*, *o*1), (*u*1, *r*, *o*2), (*u*2, *r*, *o*1), (*u*2, *r*, *o*2), (*u*2, *w*, *o*2), (*u*2, *r*, *o*3), (*u*2, *w*, *o*3)	(*u*1, *r*, *o*2), (*u*1, *w*, *o*2), (*u*2, *r*, *o*2), (*u*2, *w*, *o*2), (*u*2, *r*, *o*3), (*u*2, *w*, *o*3), (*u*2, *r*, *o*4), (*u*2, *w*, *o*4)

Table 3. List of derived privileges for the combined configurations of Figures 4a and 4b

(*u*1, *r*, *o*1), (*u*1, *w*, *o*1), (*u*1, *r*, *o*2), (*u*2, *r*, *o*1), (*u*2, *r*, *o*2), (*u*2, *w*, *o*2), (*u*2, *r*, *o*3), (*u*2, *w*, *o*3), (u2, r, o4), (u2, w, o4)

Just as access rights to perform read/write operations on resource objects are defined in terms of associations, so too are capabilities to perform administrative operations on policy elements and relations. In contrast to non-administrative access rights, where resource operations are synonymous with the access rights needed to carry out those operations (e.g., a "read" operation corresponding to an "r" access right), the authority stemming from one or more administrative access rights may be required for an administrative operation. Administrative access rights to perform an administrative operation maybe explicitly divided into two parts, as denoted by "from" and "to" suffixes.

For example, in the in context of Figure 4 we could create two associations Bob---{create ooa-from}---Bob Home and Division---{create ooa-to}---Projects, meaning that the intersection of users in Bob and Division may create "object to object attribute assignments" (ooa) from objects in Bob Home to object attributes in Projects. Remember that the set of referenced policy elements in the third term of an association (*at*) is dependent on the access rights in ars. As such, the absolute mean of the two associations is that user u2 can create assignments from o2, o3, or o4 to Projects, Project1, or Project2.

4.2.2 Prohibitions (Denies)

In addition to assignments and associations, NGAC includes three types of prohibition relations: user-deny, user attribute-deny, and process-deny. In general, deny relations specify privilege exceptions. We respectively denote a user-based deny, user attribute-based deny, and process-based deny relation by u_deny(*u*, *ars*, *pe*), ua_deny(*ua*, *ars*, *pe*), and p_deny(*p*, *ars*, *pe*), where *u* is a user, *ua* is a user attribute, *p* is a process, *ars* is an access right set, and *pe* is a policy element used as a referent for itself and the policy elements contained by the policy element. The respective meanings of these relations are that user *u*, users in *ua*, and process *p* cannot execute access rights in *ars* on policy elements in *pe*. User-deny relations and user attribute-deny relations can be created directly by an administrator or dynamically as a consequence of an obligation (see Section 4.2.3). An administrator, for example, could impose a condition where no user is able to alter their own Tax Return, in spite of the fact that the user is assigned to an IRS Auditor user attribute with capabilities to read/write all tax returns. When created through an obligation, user-deny and user attribute-deny relations can take on dynamic policy conditions. Such conditions can, for example, provide support for separation of duty policies (if a user executed capability x, that user would be immediately precluded from being able to perform capability y). In addition, the policy element component of each prohibition relation can be specified as its complement, denoted by ¬. The respective meaning of u_deny(*u*, *ars*, ¬*pe*), ua_deny(*ua*, *ars*, ¬*pe*), and p_deny(*p*, *ars*, ¬*pe*) is that the user *u*, and any user assigned to *ua*, and process *p* cannot execute the access rights in *ars* on policy elements not in *pe*.

Process-deny relations are exclusively created using obligations. Their primary use is in the enforcement of confinement conditions (e.g., if a process reads Top Secret data, preclude that process from writing to any object not in Top Secret).

4.2.3 Obligations

Obligations consist of a pair (*ep*, *r*) (usually expressed as **when** *ep* **do** *r*) where *ep* is an *event pattern* and *r* is a sequence of administrative operations, called a *response*. The event pattern specifies conditions that if matched by the context surrounding a process's successful execution of an operation on an object (an event), cause the administrative operations of the associated response to be immediately executed. The context may pertain to and the event pattern may specify parameters like the user of the process, the operation executed, and the attribute(s) of the object.

Obligations can specify operational conditions in support of history-based policies and data services.

Included among history-based policies are those that prevent leakage of data to unauthorized principals. Consider, for example the "Project Access" policy depicted in Figure 4(a). Although this policy suggests that only Group2 users can read Gr2-Secrets, data in Gr2-Secrets can indeed be leaked to Group1 users. Specifically, u2 or one of u2's processes can read o3, and subsequently write its content to o2, thereby providing u1 the capability to read the content of o3. Such leakage can be prevented with the following obligation:

When any process *p* performs (*r*, *o*) where *o*→Gr2-Secret **do**
create p-deny(*p*, {*w*}, ¬Gr2-Secret)

The effect of this obligation will prevent a process (and its user) from reading an object in Gr2-Secret and subsequently writing its content to an object in a different container (not in Gr2-Secret).

Other history-based policies include conflict of interest (if a user reads information from a sensitive data set, that user is prohibited from reading data from a second data set) and Work Flow (approving (writing to a field of)) a work item enables a second user to read and approve the work item).

4.3 NGAC Decision Function

The NGAC access decision function controls accesses in terms of processes. The user on whose behalf the process operates must hold sufficient authority over the policy elements involved. The function process_user(*p*) denotes the user associated with process *p*.

Access requests are of the form (*p*, *op*, *argseq*), where *p* is a process, *op* is an operation, and *argseq* is a sequence of one or more arguments, which is compatible with the scope of the operation. The access decision function to determine whether an access request can be granted requires a mapping from an operation and argument sequence pair to a set of access rights and policy element pairs (i.e., {(*ar*, *pe*)}) the process's user must hold for the request to be granted.

When determining whether to grant or deny an access request, the authorization decision function takes into account all privileges and restrictions (denies) that apply to a user and its processes, which are derived from relevant associations and denies, giving restrictions precedence over privileges:

A process access request (p, op, $argseq$) with mapping (op, $argseq$)→{(ar, pe)}) is granted iff for each (ar_i, pe_i) in {(ar, pe)}, there exists a privilege (u, ar_i, pe_i) where u = process_user(p), and (ar_i, pe_i) is not denied for either u or p.

In the context of Figure 4, an access request may be (p, read, o1) where p is u1's process. The pair (read, o1) maps to (r, o1). Because there exists a privilege (u1, r, o1) in table 3 and (r, o1) is not denied for u1 or p, the access request would be granted. Assume the existence of associations Division---{create ooa-to}---Projects, and Bob---{create ooa-from}---Bob Home in the context of Figure 4, and an access request (p, assign, <o4, Project1>) where p is u2's process. The pair (assign, <o4, Project1>) maps to {(create ooa-from, o4), (create ooa-to, Project1)}. Because privileges (u2, create ooa-from, o4) and (u2, create ooa-to, Project1) would exist under the assumption, and (create ooa-from, o4) and (create ooa-to, Project1) are not denied for u2 or p, the request would be granted.

4.4 Delegation

The question remains, how are administrative capabilities created? The answer begins with a superuser with capabilities to perform all administrative operations on all access control data. The initial state consists of an NGAC configuration with empty data elements, attributes, and relations. A superuser either can directly create administrative capabilities or more practically can create administrators and delegate to them capabilities to create and delete administrative privileges. Delegation and rescinding of administrative capabilities is achieved through creating and deleting associations. The principle followed for allocating access rights via an association is that the creator of the association must have been allocated the access right over the attribute in question (as well as the necessary create-assoc-from and create-assoc-to rights) in order to delegate them. The strategy enables a systematic approach to the creation of administrative attributes and delegation of administrative capabilities, beginning with a superuser and ending with users with administrative and data service capabilities.

4.5 NGAC Administrative Commands and Routines

Access requests bearing administrative operations can create and destroy basic elements, containers and relations. Each administrative operation corresponds on a one-to-one basis to an administrative routine, which uses the sequence of arguments in the access request to perform the access. Each administrative operation is carried out through one or more primitive administrative commands. NGAC defines the complete set of administrative commands and their behavior in detail. The definitions specify the preconditions that need to exist for the effect of a command to occur, and the specific effect that the command has on the contents of NGAC's Policy Information Point (policies and attributes store).

The access decision function grants the access request (and initiation of the respective administrative routine) only if the process holds all prohibition-free access rights over the items in the argument sequence needed to carry out the access. The administrative routine, in turn, uses one or more administrative commands to perform the access. Administrative commands and routines are thus the means by which policy specifications and attributes are formed.

Consider the administrative command CreateAssoc shown below, which specifies the creation of an association. The preconditions here stipulate membership of the x, y, and z parameters respectively to the user attributes (UA), access right sets (ARs), and attributes (AT) elements of the model. The body describes the addition of the tuple (x, y, z) to the set of associations (ASSOC) relation, which changes the state of the relation to ASSOC′.

```
createAssoc (x, y, z)
  $x \in UA \land y \in ARs \land z \in AT \land (x, y, z) \notin ASSOC$
    {
    $ASSOC' = ASSOC \cup \{(x, y, z)\}$
    }
```

An administrative routine consists mainly of a parameterized interface and a sequence of administrative command invocations. Each formal parameter of an administrative routine can serve as an argument in any of the administrative command invocations that make up the body of the routine. Administrative routines are used in a variety of ways. Although an administrative routine must be in place on a one-to-one basis to carry out an administrative operation, they can also be used to carry out more complex administrative tasks comprising of a sequence of administrative actions.

Consider the following administrative routine that creates a "file management" user in the context of Figure 4b. The routine assumes the pre-existence of the user attribute "Users" assigned to the "File Management" policy class shown in Figure 4b.

```
create-file-mgmt-user(user-id, user-name, user-home) {
    createUAinUA(user-name, Users);
    createUinUA(user-id, user-name);
    createOAinPC(user-home, File Management);
    createAssoc(user-name, {r, w}, user-home);
    createAssoc(user-name, {create-o-to, delete-o-from}, user-
        home);
    createAssoc(user-name, {create-ooa-from, create-ooa-to,
        delete-ooa-from, create-oaoa-from, create-oaoa-to,
        delete-oaoa-from}, user-home);
    createAssoc(user-name, {create-assoc-from, delete-assoc-
        from}, Users);
    createAssoc(user-name, {create-assoc-to, delete-assoc-to, r-
       allocate, w-allocate}, user-home);}
```

This routine with parameters (u1, *Bob* and *Bob Home*) could have been used to create "file management" data service capabilities for user u1 already in Figure 4b. Through the routine the user attribute "Bob" is created and assigned to "Users", and user u1 is created and assigned to "Bob". In addition, the object attribute "Bob Home" is created and assigned to policy class "File Management". In addition, user u1 is delegated administrative capabilities to create, organize, and delete object attributes (presented folders) in Bob Home, and u1 is provided with capabilities to create, read, write, and delete objects that correspond to files and place those files into his folders. Finally, u1 is provided with discretionary capabilities to "grant" to other users in the "Users" container capabilities to perform read/write operations on individual files or to all files in a folder in his

Home.

4.6 Arbitrary Data Service Operations

NGAC recognizes administrative operations for the creation and management of its data elements and relations that represent policies and attributes, and basic input and output operations (e.g., read and write) that can be performed on objects that represent data service resources. In accommodating data services, NGAC may establish and provide control over other types of operations, such as send, submit, approve, and create folder. However, it does not necessarily need to do so. This is because the basic data service capabilities to consume, manipulate, manage, and distribute access rights on data can be attained as combinations of read/write operations on data and administrative operations on data elements, attributes, and relations. For example, the create-file-mgmt-user routine specified above provides a user with capabilities to create and manage files and folders, and control and share access to objects in the user's home directory.

4.7 NGAC Functional Architecture

NGAC's functional architecture (shown in Figure 5), like XACML's, encompasses four layers of functional decomposition: Enforcement, Decision, Administration, and Access Control Data, and involves several components that work together to bring about policy-preserving access and data services.

Among these components is a PEP that traps application requests. An access request includes a process id, user id, operation, and a sequence of one or more operands mandated by the operation that pertain to either a data resource or an access control data element or relation. Administrative operational routines are implemented in the PAP and read/write routines are implemented in the RAP.

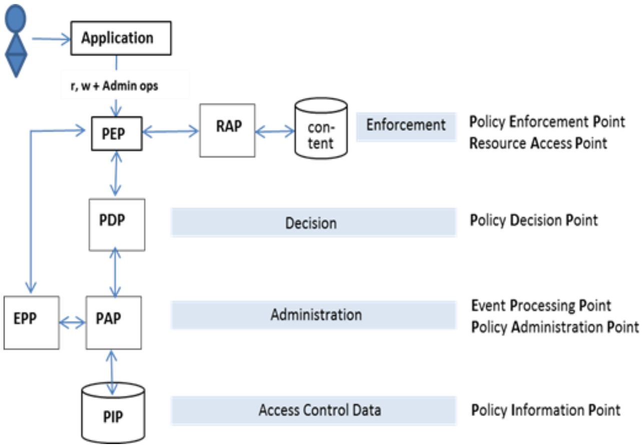


Figure 5: NGAC Standard Functional Architecture

To determine whether to grant or deny, the PEP submits the request to a PDP. The PDP computes a decision based on current configuration of data elements and relations stored in the PIP, via the PAP. Unlike the XACML architecture, the access request information from an NGAC PEP together with the NGAC relations (selectively retrieved by the PDP) provide the full context for arriving at a decision. The PDP returns a decision of grant or deny to the PEP. If access is granted and the operation was read/write, the PDP also returns the physical location where the object's content resides, the PEP issues a command to the appropriate RAP to execute the operation on the content, and the RAP returns the status. In the case of a read operation, the RAP also returns the data type of the content (e.g., PowerPoint) and the PEP invokes the correct data service application for its consumption. If the request pertained to an administrative operation and the decision was grant, the PDP issues a command to the PAP for execution of the operation on the data element or relation stored in the PIP, and the PAP returns the status to the PDP, which in turn relays the status to the PEP. If the returned status by either the RAP or PAP is "successful", the PEP submits the context of the access to the Event Processing Point (EPP). If the context matches an event pattern of an obligation, the EPP automatically executes the administrative operations of that obligation, potentially changing the access state. Note that NGAC is data type agnostic. It perceives accessible entities as either data or access control data elements or relations, and it is not until after the access process is completed that the actual type of the data matters to the application.

5. COMPARISON OF XACML AND NGAC

XACML is similar to NGAC insofar as they both provide flexible, mechanism-independent representations of policy rules that may vary in granularity, and they employ attributes in computing decisions. However, XACML and NGAC differ significantly in their expression of policies, treatment of attributes, computation of decisions, and representation of requests. In this section, we analyze these similarities and differences with respect to the degree of separation of access control logic from proprietary operating environments and four ABAC considerations identified in NIST SP 800-162: operational efficiency, attribute and policy management, scope and type of policy support, and support for administrative review and resource discovery. For the purposes of comparison we normalize some XACML and NGAC terminology.

5.1 Separation of Access Control Logic from Operating Environments

Both XACML and NGAC achieve separation of access control logic of data services from proprietary operating environments, but to different degrees. XACML's separation is partial. XACML does not envisage the design of a PEP that is data service agnostic. An XACML deployment consists of one or more data services, each with an operating environment-dependent PEP, and operating environment-dependent operational routines and resource types, that share a common PDP and access control information consisting of policies and attributes. In other words, a PEP under the XACML architecture is tightly coupled to a specific operating environment for which it was designed to enforce access.

The degree of separation that can be achieved by NGAC is near complete. Although an NGAC deployment could include a PEP with an Application Programming Interface (API) that recognizes operating environment-specific operations (e.g., send and forward operations for a messaging system), it does not necessarily need to do so. NGAC includes a standard PEP with an API that supports a set of generic, operating environment-agnostic operations (read, write, create, and delete policy elements and relations). This API enables a common, centralized PEP to be implemented to serve the requests of multiple applications. Although the generic operations may not meet the requirements of every application (e.g., transactions that perform computations on attribute values), calls from many applications can be accommodated. This includes operations that generically pertain to consumption, alteration, management, and sharing of data resources. As a consequence, NGAC can completely displace the need for an access control mechanism of an operating environment in that through the same

PEP API, set of operations, access control data elements and relations, and functional components, arbitrary data services can be delivered to users, and arbitrary, mission-tailored access control policies can be expressed and enforced over executions of application calls.

5.2 Operational Efficiency

An XACML request is a collection of attribute name, value pairs for the subject (user), action (operation), resource, and environment. XACML identifies relevant trusted and untrusted access policies and rules for computing decisions through a search for Targets (conditions that match the attributes of the request). Because multiple Policies in a PolicySet and/or multiple Rules in a Policy may produce conflicting access control decisions, XACML resolves these differences by applying collections of potentially several rule and policy combining algorithms. If the attributes are not sufficient for the evaluation of an applicable rule, the PDP may search for additional attributes. The entire process involves converting a PEP request into an XACML canonical form, collecting attributes, matching target conditions, computing rules, (optionally) issuing administrative requests (for determining a chain of trust for applicable untrusted access policies), resolving conflicts, and converting an XACML access decision to a PEP specific response, involving at least two data stores.

NGAC is inherently more efficient. An NGAC request is composed of a process id, user id, operation, and a sequence of one or more operands mandated by the operation that affects either a resource or access control data. NGAC identifies relevant policies, attributes and prohibitions, by reference (through relations) when computing a decision. Like XACML, NGAC combines policies. However, it does not compute and then combine multiple local decisions, but rather takes multiple policies into consideration when determining the existence of an appropriate privilege. All information necessary in computing an access decision resides in a single database. NGAC does not include a context handler for converting requests and decisions to and from its canonical form or for retrieving attributes. Although considered a component of its access control process, obligations do not come into play until after a decision has been rendered and data has been successfully altered or consumed.

5.3 Attribute and Policy Management

Because XACML is implemented in XML, it inherits XML's benefits and drawbacks. The flexibility and expressiveness of XACML, while powerful, make the specification of policy complex and verbose [12]. Applying XACML in a heterogeneous environment requires fully specified data type and function definitions that produce a lengthy textual document, even if the actual policy rules are trivial. In general, platform-independent policies expressed in an abstract language are difficult to create and maintain by resource administrators [14]. Unlike XACML, NGAC is a relations-based standard, which avoids the syntactic and semantic complexity in defining an abstract language for expressing platform-independent policies [12]. NGAC policies are expressed in terms of configuration elements that are maintained at a centralized point and typically rendered and manipulated graphically. For example, to describe hierarchical relations and inheritance properties of attributes, NGAC requires only the addition of links representing assignment relations between them; in XACML, relations need to be inserted in precise syntactic order.

XACML's ability to specify policies as logical conditions provides policy expression efficiency. Consider the XACML Policy specified in Section 3.4 and the attribute names, values and value assignments in table 1. NGAC could express this same policy and authorization state using enumerated attributes, assignments, and associations. See [21] for a detailed configuration. The NGAC eqivelent policy would include five association relations, while XACML uses just three rules. As the number of Wards that are considered by the policy increases, so will the number of NGAC association relations, but the number of XACML rules will always remain the same. Recognize that for this policy, the number of attributes and attribute assignments will always be the same for XACML and NGAC regardless of the number of Wards considered. On the other hand, for some policies, the number of XACML attribute assignments can far exceed those necessary for an NGAC equivalent policy. Consider the TCSEC MAC Policy [3, 5] expressed using XACML rules and NGAC relations. For the XACML TCSEC MAC policy to work (using static rules), all resources whether classified or unclassified are required to be assigned to attributes to prevent classified data from being leaked to unclassified data. For the NGAC TCSEC MAC policy to work (using obligations (e.g., **when** any process p performs (read, o) where o→Top Secret **do** create p-deny(p, {write}, ¬Top Secret)), only objects that are actually classified (e.g., Secret and Top Secret) are required to be assigned to attributes. See [21] for detailed XACML and NGAC expressions of the TCSEC MAC policy.

Proper enforcement of data resource policies is dependent on administrative policies. This is especially true in a federated or collaborative environment, where governance policies require different organizational entities to have different responsibilities for administering different aspects of policies and their dependent attributes.

XACML and NGAC differ dramatically in their ability to impose policy over the creation and modification of access control data (attributes and policies). NGAC manages attributes and policies through a standard set of administrative operations, applying the same enforcement interface and decision making function as it uses for accessing data resources. XACML does not recognize administrative operations, but instead manages policy content through a Policy Administration Point (PAP) with an interface that is different from that for accessing data resources. XACML provides support for decentralized administration of some of its access policies. However the approach is only a partial solution in that it is dependent on trusted and untrusted policies, where trusted policies are assumed valid, and their origin is established outside the delegation model. Furthermore, the XACML delegation model does not provide a means for imposing policy over modification of access policies, and offers no direct administrative method for imposing policy over the management of its attributes.

NGAC enables a systematic and policy-preserving approach to the creation of administrative roles and delegation of administrative capabilities, beginning with a single administrator and an empty set of access control data, and ending with users with data service, policy, and attribute management capabilities. NGAC provides users with administrative capabilities down to the granularity of a single configuration element, and can deny users administrative capabilities down to the same granularity.

5.4 Scope and Type of Policy Support

Although data resources may be protected under a wide variety of different access policies, these policies can be generally categorized as either discretionary or mandatory controls. Discretionary access control (DAC) is an administrative policy that permits system users to allow or disallow other users' access to objects that are placed under their control [15]. Although XACML can theoretically implement DAC policies, it is not efficient. Consider the propagation feature of DAC. DAC permits owners/creators of objects to grant some or all of their capabilities to other users, and the grantees can further propagate those capabilities on to other users. The overall DAC feature to grant privileges to another user and the ability of the grantee to propagate those privileges cannot be supported in XACML syntax using "Access Policies" alone.

Therefore, all the capabilities of the owner/creator of an object together with administrative capabilities to grant those privileges have to be specified using a Trusted Administrative policy. The capabilities held by owner/creator can be captured by designating the owner/creator of the object as the "access-subject", and the administrative capability to grant privileges to others can be captured by designating the owner/creator as a delegate in that policy type. The creation of this trusted administrative policy enables creation of derived administrative policies with the owner/creator as the policy issuer with the specified set of capabilities. The specification of a "delegate" in this derived administrative policy (not trusted) provides a means for the owner/creator to grant capabilities to other users, as well as the ability for the grantee to propagate those capabilities to other users. However, while it is theoretically possible to implement DAC by leveraging XACML's delegation feature, this approach involves significant administrative overhead. The solution requires the specification of a trusted administrative policy and a set of derived administrative policies for every object owner/creator, and for all grantees of the capabilities.

Conversely, NGAC has a flexible means of providing users with administrative capabilities to include those necessary for the establishment of DAC policies, as shown in section 5.4.

In contrast to DAC, mandatory access control (MAC) enables ordinary users' capabilities to execute resource operations on data, but not administrative capabilities that may influence those capabilities. MAC policies unavoidably impose rules on users in performing operations on resource data. MAC policies can be further characterized as controls that accommodate confinement properties to prevent indirect leakage of data to unauthorized users, and those that do not.

Expression of non-confinement MAC policies is perhaps XACML's strongest suit. XACML can specify rules and other conditions in terms of attribute values of varying types. There are undoubtedly certain policies that are expressible in terms of these rules that cannot be easily accommodated by NGAC. This is especially true when treating attribute values as integers. For example, to approve a purchase request may involve adding a person's credit limit to their account balance. Furthermore, XACML takes environmental attributes into consideration in expressing policy, and NGAC does not. However, there are some non-confinement MAC properties, such as a variety of history-based policies that NGAC can express, and XACML cannot. Although XACML has been shown to be capable of expressing aspects of standard RBAC [1] through an XACML profile [16], the profile falls short of demonstrating support for dynamic separation of duty, a key feature used for accommodating the principle of least privilege, and separation of duty, a key feature for combatting fraud. Annex B of Draft standard Next Generation Access Control – Generic Operations and Data Structures (NGAC-GOADS) [20] demonstrates NGAC support for all aspects of the RBAC standard.

In addition to static and dynamic separation of duty, NGAC has shown support for history-based separation of duty [7]. In their seminal paper on the subject [19], Simon and Zurko describe history-based separation of duty as the most accommodating form of separation of duty, subsuming the policy objectives of other forms.

In contrast to NGAC, XACML does not recognize the capabilities of a process independent of the capabilities of its user. Without such features, XACML is ill equipped to support confinement and as such is arguably incapable of enforcement of a wide variety of policies. These confinement-dependent policies include some instances of role-based access control (RBAC), e.g., "only doctors can read the contents of medical records", originator control (ORCON) [10] and Privacy, e.g., "I know who can currently read my data or personal information", conflict of interest [4], e.g., "a user with knowledge of information within one dataset cannot read information in another dataset", or Multi-level Security [3]. [5]. Through imposing process level controls in conjunction with obligations, NGAC has shown [7] support for these and other confinement-dependent MAC controls.

5.5 Administrative Review and Resource Discovery

A desired feature of access controls is review of capabilities (*op*, *o*) of users and access control entries (*u*, *op*) of objects, where *u* is a user, *op* is an operation, and *o* is an object [15] [11]. These features are often referred to as "before the fact audit" and resource discovery. "Before the fact audit" is one of RBAC's most prominent features [18]. Being able to discover or see a newly accessible resource is an important feature of any access control system. NGAC supports efficient algorithms for both per-user and per-object review. Per-object review of access control entries is not as efficient as a pure access control list (ACL) mechanism, and per-user review of capabilities is not as efficient as that of RBAC. However, this is due to NGAC's consideration of conducting review in a multi-policy environment. NGAC can efficiently support both per-object and per-user reviews of combined policies, where RBAC and ACL mechanisms can do only one type of review efficiently, and rule-based mechanisms such as XACML, although able to combine policies, cannot do either efficiently. In other words, there exists no method of determining the authorization state without testing all possible decision outcomes.

6. REFERENCES

[1] Information technology – Role-Based Access Control (RBAC), INCITS 359-2004, American National Standard for Information Technology, American National Standards Institute, 2004.

[2] Information technology - Next Generation Access Control - Functional Architecture (NGAC-FA), INCITS 499-2013, American National Standard for Information Technology, American National Standards Institute, March 2013.

[3] D. Bell and L. La Padula. Secure computer systems: unified

exposition and MULTICS. Report ESD-TR-75-306, The MITRE Corporation, Bedford, Massachusetts, March 1976.

[4] D.F.C. Brewer and M.J. Nash, “The Chinese Wall Security Policy,” 1989 IEEE Symposium on Security and Privacy, Oakland, California, USA, May 1-3, 1989, pp. 206-214. http://dx.doi.org/10.1109/SECPRI.1989.36295 [accessed 11/15/15]

[5] DoD Computer Security Center, Trusted Computer System Evaluation Criteria (December 1985).

[6] D.F. Ferraiolo, S.I. Gavrila, V.C. Hu, and D.R. Kuhn, “Composing and Combining Policies Under the Policy Machine,” Tenth ACM Symposium on Access Control Models and Technologies (SACMAT ‘05), Stockholm, Sweden, 2005, pp. 11-20.

[7] D.F. Ferraiolo, V. Atluria, and S.I. Gavrila, “The Policy Machine: A Novel Architecture and Framework for Access Control Policy Specification and Enforcement,” Journal of Systems Architecture, vol. 57, no. 4, pp. 412-424, April 2011. http://dx.doi.org/10.1016/j.sysarc.2010.04.005 [accessed 11/15/15]

[8] D. Ferraiolo, S. Gavrila, and W. Jansen, National Institute of Standards and Technology (NIST) IR-7987 Revision 1, “Policy Machine: Features, Architecture, and Specification,” October 2015. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7987r1.pdf

[9] D. Ferraiolo, S. Gavrila, and W. Jansen, “On the Unification of Access Control and Data Services,” in Proc. IEEE 15th International Conference of Information Reuse and Integration, 2014, pp. 450 – 457. http://csrc.nist.gov/pm/documents/ir2014_ferraiolo_final.pdf

[10] R. Graubart, On the need for a third form of access control, in: Proc. National Computer Security Conference, 1989, pp. 296 –304.

[11] V.C. Hu, D.F. Ferraiolo, and D.R. Kuhn, National Institute of Standards and Technology (NIST) Interagency Report (IR) 7316, “Assessment of Access Control Systems,” September 2006. http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

[12] V. C. Hu, D.F. Ferraiolo, and K. Scarfone, Access Control Policy Combinations for the Grid Using the Policy Machine, Cluster Computing and the Grid, 2007, pp. 225-232.

[13] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, National Institute of Standards and Technology (NIST) SP-800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

[14] M. Lorch et al, “First Experience Using XACML for Access Control in Distributed Systems, ACM Workshop on XML Security, Fairfax, Virginia, 2003.

[15] Guide to Understanding Discretionary Access Control in Trusted Systems, NCSC-TG-003, Version-1, National Computer Security Center, Fort George G. Meade, USA, September 30, 1987, 29 pp. http://csrc.nist.gov/publications/secpubs/rainbow/tg003.txt

[16] XACML Profile for Role Based Access Control (RBAC), Committee Draft 01, February 2004.

[17] The eXtensible Access Control Markup Language (XACML), Version 3.0, OASIS Standard, January 22, 2013. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf

[18] 2010 Economic Analysis of Role-Based Access Control, RTI Number 0211876, Research Triangle Institute, December 2010.

[19] R. Simon, M. Zurko, Separation of duty in role based access control environments, Proc. New Security Paradigms Workshop, 1997.

[20] Information technology – Next Generation Access Control – Generic Operations and Data Structures, INCITS 526, American National Standard for Information Technology, American National Standards Institute, to be published.

[21] D. F. Ferraiolo, R. Chandramouli, V. Hu, and R. Kuhn, National Institute of Standards and Technology DRAFT (NIST) SP-800-178, A Comparison of Attribute Based Access Control (ABAC) Standards for Data Services, December 2015. http://csrc.nist.gov/publications/drafts/800178/sp800_178_draft.pdf

2 Volt Pulse-Driven Josephson Arbitrary Waveform Synthesizer

Nathan E. Flowers-Jacobs, Alain Rüfenacht, Anna E. Fox, Paul D. Dresselhaus, Samuel P. Benz

National Institute of Standards and Technology, Boulder, CO 80305, USA
nathan.flowers-jacobs@nist.edu

***Abstract* — We created a Josephson Arbitrary Waveform Synthesizer (JAWS) with a root-mean-square (rms) output magnitude of 2 V. This system is composed of two 1 V chips operating on a cryocooler. By controlling the relative phase of the two chips' output voltage, we add the voltages in quadrature and create rms output voltages between (1+1) V=2 V and (1-1) V=0 V. We use this control to compare the two halves of the system as a function of the relative phase, and measure a difference of 8 parts in 10^8 at a nominal rms amplitude of 1 V and 1 kHz.**

***Index Terms* —Digital-analog conversion, Josephson junction arrays, Measurement standards, Signal synthesis, Superconducting integrated circuits, Voltage measurement.**

I. Introduction

The pulse-driven Josephson Arbitrary Waveform Synthesizer (JAWS), also known as the AC Josephson Voltage Standard (ACJVS), was invented in 1995 [1]. In the ensuing years, an important goal has been to increase the rms output of the quantum-accurate waveforms synthesized by this Josephson junction (JJ) based digital-to-analog convertor. Audio-frequency voltage calibrations that are performed with thermal voltage converters and impedance measurements, along with other precision measurements, would benefit from rms output voltages above 2 V. The most sensitive range of the converters extends up to 10 V, and a larger output voltage would increase the signal-to-noise ratio of other measurements. JAWS systems with a rms output voltage of 1 V have been demonstrated in the past two years [2]-[4].

We recently implemented a new 2 V JAWS system that combines two 1 V chips on a cryocooler and has an operating current range greater than 1 mA [5]. The two chips are connected in series at cryogenic temperatures using a short copper wire. Each chip is driven by a separate custom, large-memory pulse generator [6]. Further details of the design and operation of this 2 V JAWS system are described in [5].

In this paper, we report for the first time preliminary results of a comparison between two halves of the 2 V JAWS system. Since the two chips are driven with pulses from two separate generators, we can choose to generate waveforms with arbitrary phases (and magnitudes). In particular, this allows us to perform a precision null measurement by generating waveforms that have precisely identical rms magnitudes of 1 V, but are exactly 180° out of phase.

II. JAWS Comparison

In Fig. 1 we show the digitized output of the JAWS system generating a 1 kHz waveform with a rms magnitude of 2.0000 V. With this large output voltage, we observe harmonics that are -123 dBc (decibels below the carrier/fundamental frequency), which are due to nonlinearities in the digitizer [2].

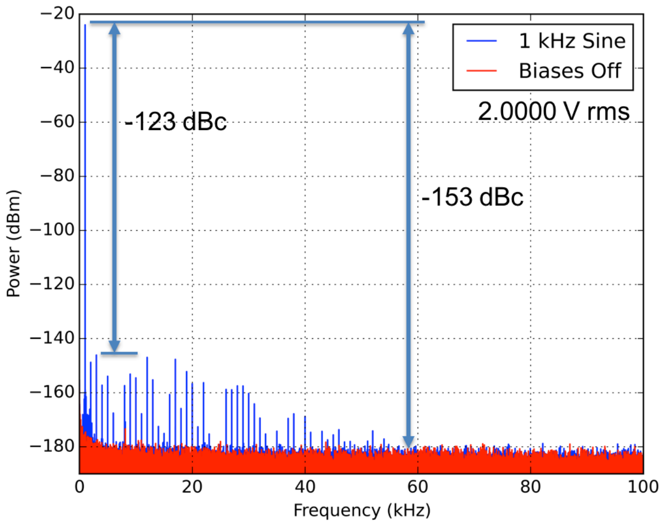


Fig. 1. Digitally sampled spectral measurements showing a low distortion JAWS output voltage with an rms magnitude of (1+1) V = 2 V (blue), and background noise floor without any JAWS pulses (red). The digitizer was set to its 10 V range with a 1 MΩ input impedance and a sampling rate of 10^6 samples/s. We plot the phase-coherent average of 4 data sets, each taken with a 2 Hz resolution bandwidth.

To generate this calculable voltage from the two chips, we must first synchronize the two pulse generators. We start by loading both pulse generators with the same pulse pattern and then tuning the relative delay between the generators. We have arbitrary control over the delay with a fine time step of 70 ps, which is equal to the width of a single pulse. This phase control is displayed in Fig. 2, where we sweep the relative phase between the two generators over 360° and measure the quadrature sum of the 1 kHz waveforms generated by the two chips. Achieving a precision null requires removing a time delay of 111 ns, which is the result of delays in the trigger system and other asymmetries in the two driving circuits. We synchronize the two generators by compensating for this time delay.

We also use the depth of the precision cancellation to place a limit on the difference in the output voltages of the two 1 V chips (similar to [7]) due to any systematic errors. In Fig. 3 we plot the spectrum of the cancelled waveform, that is, the precision null. Each chip is generating a voltage at 1 kHz with an rms magnitude of 1 V, but with a 180° relative phase shift

U.S. Government work not protected by U.S. copyright

Flowers-Jacobs, Nathan; Rufenacht, Alain; Fox, Anna; Dresselhaus, Paul; Benz, Samuel.
"2 V Pulse-Driven Josephson Arbitrary Waveform Synthesizer."
Paper presented at the CPEM 2016 Conference, Ottawa, Canada, Jul 10-Jul 15, 2016.

(to within 70 ps). The precision null has a residual voltage at the fundamental frequency with an rms magnitude of 82 nV. We also observe a harmonic of the fundamental that is -165 dBc (relative to an assumed in-phase carrier with an rms magnitude of 2 V).

Possible explanations for the residual voltage are as follows: (1) differences in pulse arrival time at and within each array; (2) insufficient fine tuning of the relative phase shift between the arrays; and (3) systematic-error voltage signals related to compensation currents driving each JJ array. The small magnitude of the error voltage and the short 70 ps pulse width influence the likelihood of some of these explanations relative to others. This error is interesting and shows the importance of investigating the systematic errors through flat spot measurements for all bias parameters and their phase delays.

III. Conclusion

We evaluated the relative performance of the two chips that make up our new 2 V ACJVS system [5]. We observed that the relative error between the two halves of the system is of the order of 8 parts in 10^8, with each half generating a 1 kHz waveform with an output rms magnitude of 1 V. In the future, we intend to extend this comparison to other frequencies and present an analysis of systematic errors.

Acknowledgement

We thank Steve Waltman for creating the custom pulse generators, Robert Schwall for cryocooler development, Michael Elsbury and Zoya Popović for microwave design, and the Boulder Microfabrication Facility for chip fabrication.

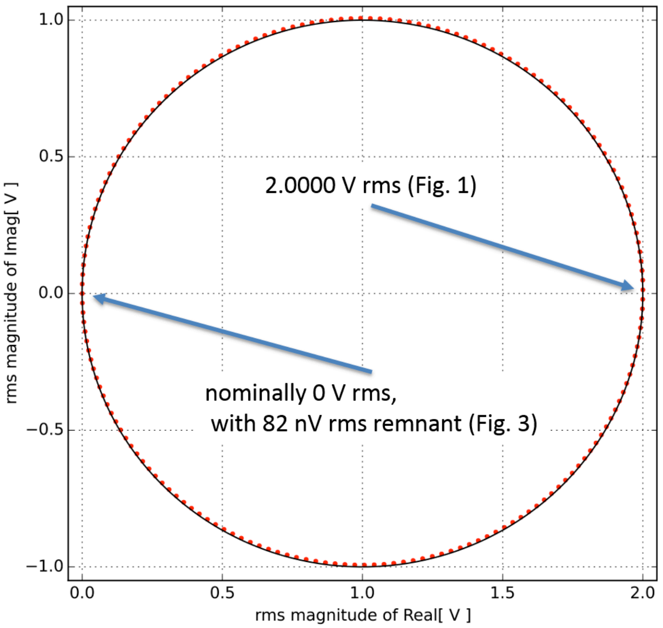


Fig. 2. Measured complex rms magnitude of fundamental tone at 1 kHz with a relative phase shift of 2° between data points, and theoretical expectation (line, no fit parameters).

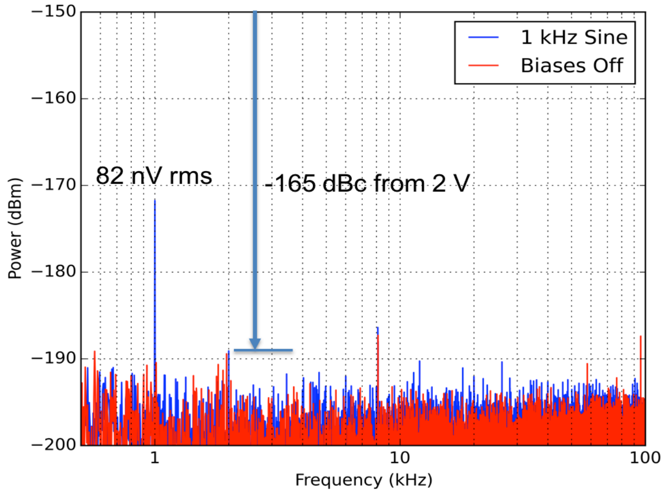


Fig. 3. Digitally sampled spectral measurement showing a low distortion JAWS output voltage with an rms magnitude of (1-1) V = 0 V with 82 nV remnant (blue), and background noise floor without any JAWS pulses (red). The digitizer was set to its 2 V range with a 1 MΩ input impedance and a sampling rate of 10^6 samples/s. We plot the phase-coherent average of 16 data sets, each taken with a 2 Hz resolution bandwidth.

References

[1] S. P. Benz and C. A. Hamilton, "A pulse-driven programmable Josephson voltage standard," *Appl. Phys. Lett.*, vol. 68, pp. 3171-3173, May 1996.

[2] S. P. Benz, S. B. Waltman, A. E. Fox, P. D. Dresselhaus, A. Rüfenacht, J. M. Underwood, L. A. Howe, R. E. Schwall, and C. J. Burroughs, "One-Volt Josephson Arbitrary Waveform Synthesizer," *IEEE Trans. Appl. Supercond.*, vol. 25, no. 1, Feb. 2015, Art. ID 1300108.

[3] S. P. Benz, S. B. Waltman, A. E. Fox, P. D. Dresselhaus, A. Rüfenacht, L. Howe, R. E. Schwall, and N. E. Flowers-Jacobs, "Performance Improvements for the NIST 1 V Josephson Arbitrary Waveform Synthesizer," *IEEE Trans. Appl. Supercond.*, vol. 25, no. 3, June 2015, Art. ID 1400105.

[4] O. F. Kieler, R. Behr, R. Wendisch, S. Bauer, L. Palafox, and J. Kohlmann, "Towards a 1 V Josephson Arbitrary Waveform Synthesizer," *IEEE Trans. Appl. Supercond.*, vol. 25, no. 3, June 2015, Art. ID 1400305.

[5] N E. Flowers-Jacobs, A. E. Fox, P. D. Dresselhaus, R. E. Schwall, and S. P. Benz, "Two-Volt Josephson Arbitrary Waveform Synthesizer," to be submitted to *IEEE Trans. Appl. Supercond.*

[6] S. P. Benz and S. B. Waltman, "Pulse-bias electronics and techniques for a Josephson arbitrary waveform synthesizer," *IEEE Trans. Appl. Supercond.*, vol. 24, no. 6, Dec. 2014, Art. ID 1400107.

[7] O. F. Kieler, R. Behr, D. Schleussner, L. Palafox, and J. Kohlmann, "Precision Comparison of Sine Waveforms With Pulse-Driven Josephson Arrays," *IEEE Trans. Appl. Supercond.*, vol. 23, no. 3, June 2013, Art. ID 1301404.

Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 45 (2016) 131 – 134

www.elsevier.com/locate/procedia

3rd CIRP Conference on Surface Integrity (CIRP CSI)

Effect of process parameters on the surface roughness of overhanging structures in laser powder bed fusion additive manufacturing

Jason C. Fox[a]*, Shawn P. Moylan[a], Brandon M. Lane[a]

[a]National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20886, USA

* Corresponding author. Tel.: +1-301-975-2171 ; fax: +1-301-975-8058. *E-mail address:* jason.fox@nist.gov

Abstract

The development of additive manufacturing has allowed for increased flexibility and complexity of designs over formative and subtractive manufacturing. However, a limiting factor of additive manufacturing is the as-built surface quality as well as the difficulty in maintaining an acceptable surface roughness in overhanging structures. In order to optimize surface roughness in these structures, samples covering a range of overhang angles and process parameters were built in a laser powder bed fusion system. Analysis of the surface roughness was then performed to determine a relationship between process parameters, angle of the overhanging surface, and surface roughness. It was found that the analysis of surface roughness metrics, such as *Rpc*, *Rsm*, and *Rc*, can indicate a shift between surfaces dominated by partially melted powder particles and surfaces dominated by material from the re-solidified melt track.

Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the scientific committee of the 3rd CIRP Conference on Surface Integrity (CIRP CSI)

Keywords: Selective Laser Melting (SLM); Roughness; Overhangs

1. Introduction

Additive manufacturing (AM) is a layer by layer process that fabricates parts directly from a 3-D digital model. This is accomplished by slicing the model into layers to create 2-D cross sections that the equipment can use as build instructions. Laser Powder Bed Fusion (L-PBF), for example, will fabricate a part by spreading a thin layer of powder (20 µm to 100 µm) across a build platform and using a high power laser to selectively melt regions of that layer. Once the layer is melted, the build platform lowers, new powder is spread across the build platform, and the process repeats until the build is complete.

A key advantage to AM over formative (e.g., casting) or subtractive (e.g., milling) methods is the ability to produce highly complex shapes. However, a limiting factor in AM is the as-built quality of surfaces. Methods exist to process surfaces after a part has been built [1,2] and during the build process through laser re-melting [3] and pulse shaping [4], but as the complexity of parts increases, the ability to successfully post-process the surface decreases [5]. As such, the as-built surface quality of a part has been cited as a key need for AM [6].

The surface roughness of AM parts has been the focus of several studies. Mumtaz and Hopkinson performed a full factorial analysis of the top and side surface roughness of multilayer thin-wall Inconel 625 parts, finding that parameter changes that tend to decrease roughness on one surface increase it on the other and optimization of the surface roughness requires a thorough understanding of how changes in process parameters affect different aspects of the part [7]. Strano *et al.* investigated the effect of surface angle on roughness for upward-facing surfaces in 316L steel [8]. Diatlov analysed parts with a wide range of surface slopes and found potential for analysis of the spectrum of the surface profile parameter *Ra* to determine surface characteristics [9]. Jamshidinia and Kovacevic found that an increase in heat accumulated during the build of thin-walled structures increases the surface roughness through an increase in adherence of partially melted powder particles to the part surface [10].

Triantaphyllou *et al.* investigated the upward- and downward-facing surface roughness for varying angles, compared results from multiple measurement instruments, and found that the *Ssk* parameter can be used for differentiating between upward- and downward-facing surfaces [11]. Aside

2212-8271 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the scientific committee of the 3rd CIRP Conference on Surface Integrity (CIRP CSI)

doi:10.1016/j.procir.2016.02.347

from this, however, little research has been performed to characterize downward-facing surface roughness, which is often the highest roughness [12]. Additionally, there is a lack of understanding of how and when structures that characterize the surface occur and how they affect the measured surface roughness parameters.

There is a wide range of mechanisms that contributes to the roughness of an AM surface, including both the process input parameters as well as the complex physical processes that occur during melting and solidification of the metal powder [13]. Understanding of surface characteristics is required in determining their effects on fatigue properties and in designing parts with improved performance [6]. Additionally, surface roughness has the potential to be used as a process signature. A strong quantitative understanding of relationships between measured surface parameters and the surface characteristic causing variation in measurements can determine if defects stem from AM system condition and performance or necessary maintenance (such as beam focus adjustments).

The purpose of this research is to understand the relationship between surface roughness parameters and the contributing surface features as a function of beam power, travel velocity, and overhang angle.

2. Experimental procedure

Experiments were performed on the EOS M270[1] system at the National Institute of Standards and Technology (NIST) using the commercially available EOS StainlessSteel GP1 (corresponds to US classification 17-4 [14]). It should be noted that the material used for the build was powder reclaimed from prior builds using an 80 µm sieve. It is assumed that the condition of the powder can have a large effect on the surface quality of parts being built and analysis of the powder is currently underway. All parts were fabricated during the same build. Thus, while the specific details of the powder have not yet been determined, the powder conditions are consistent across all of the samples.

The parts were designed as parallelepipeds with varying angles of overhang (α) to determine the effect of overhang angle on the surface roughness of the downward-facing surface. Fig. 1 shows an example model of the parallelepiped with a 60˚ angle overhang (α = 60˚). Analysis was performed on overhang angles of 30˚, 45˚, 60˚, and 75˚ as measured from the build plane. Prior experience has shown that the 30˚ overhang would build poorly (or crash the build) if it were built without supporting structures. To avoid this problem, hatched supports were added beneath the overhang. A 1 mm wide strip down the centre of the overhanging surface was left unsupported to allow measurement of the as-built surface.

To assess the effect of process parameters on surface characteristics, contour parameters with varying beam power and travel velocity were chosen in order to cover a wide range of the process space. Selection of process parameters can be seen in Table 1.

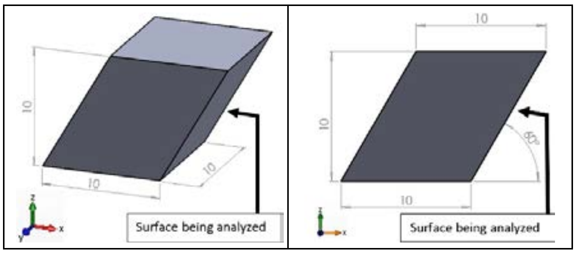


Fig. 1. Model parallelepiped for surface characterization, where α=60°. Dimensions are in millimeters. Build direction is positive z.

Table 1. Process parameters for experiments.

Line Energy - *P/v* (J/m)	Power (W)	Velocity (mm/s)	Contour Number
13.3	40	3000	1
35.7	25	700	2
46.7	140	3000	3
57.1	40	700	4
65	195	3000	5
71.4	25	350	6
114.3	40	350	7
116.4	195	1675	8
278.6	195	700	9

For each contour parameter set, parallelepipeds for each angle were built creating a total of 36 samples. To minimize the effect of incident angle of the laser beam and positional dependency on the build platform [15], all samples were positioned equidistant from the center of the build platform with the down-facing surface forming a straight line to the center of the beam source.

3. Analysis methods

Surface characterization was performed using a white light interferometer, described in detail in [16], and 10x objective lens. Using white light interferometry to analyze a very rough surface is a challenge due to difficulty in achieving null fringe condition (perfect leveling of the sample surface being measured). Because of this, a diamond-turned aluminum disk was first used to level the sample platform prior to any measurements. Thus, leveling the surface was performed as best as possible assuming that the surface being measured and the surface laying on the platform are parallel. This leveling procedure was performed before each measurement session to maintain a consistent leveling for each sample and prevent deviations due to errors caused by the leveling of the samples.

To create a large enough measurement of the sample surface to properly perform digital Gaussian filtering based on the ISO 4287 standard [17], nine images with 20 percent overlap were taken vertically down the downward-facing surface (in the build direction) and stitched together to create an

[1] Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

approximately 8 mm long measurement. The values presented used a bandpass digital Gaussian filter with a short cut-off length of 25 μm and a long cut-off length of 0.8 mm. The filtering process results in an evaluation length equal to five long cut-off lengths, or 4 mm. These filters are defined by ISO 4287 and represent a common practice in AM surface roughness research [18].

Scanning electron microscope (SEM) images were also taken for qualitative analysis of select surfaces.

4. Results

4.1. Qualitative Analysis

SEM images for two of the α = 60˚ samples can be seen in Fig. 2. Fig. 2a) shows the downward-facing surface of the sample built with contour parameter set 4 and Fig. 2b) shows the downward-facing surface of the sample built with contour parameter set 9. From these images there is a clear difference in the structures that characterize the surface. In Fig. 2a) the surface is dominated by the adherence of partially melted powder particles, between which the solidified material of the part can be seen. In Fig. 2b) the adherence of partially melted powder particles is less prevalent and more of the solidified material of the part can be seen.

Material that has been deformed by the recoater blade (the mechanism for spreading powder across the build area) can be seen in Fig. 2b). The increased power that is being used for contour parameter set 9 could be creating several factors that result in the part impacting the recoater blade. Residual stress can cause the part to warp into the path of the recoater blade. An increase in the height of consolidated material, as seen by Yasa *et al.* [19] and Yadroitsev and Smurov [20], can be above the height of the new layer. Additionally, impact with the recoater blade could be caused by a combination of these two (or other) factors.

The challenge is to determine surface parameters that can discern these varying features.

4.2. Quantitative Analysis

Analysis of *Ra* values can be seen in Fig. 3, which shows a clear dependence of surface angle on *Ra*. As α decreases, the value of *Ra* increases, which is expected and consistent with previous results [11]. However, it is also expected that the parametric analysis presented in this research would contain a relationship to *Ra* and a clear connection has not yet emerged. The results seen in Fig. 3 show that there is not a clear dependency on process parameters. Although not presented, this was also true of *Rq*, *Rz*, *Rt*, *Rp*, *RΔq*, and *Rsk*. Additional qualitative analysis to determine specific surface features caused by changes in process parameters is required to determine a relationship between process parameters and roughness parameters.

While the increase in *Ra* with decreasing α is an expected result, *Ra* does not yet provide a quantitative understanding of the specific surface characteristics seen in the qualitative analysis. One characteristic, however, can be seen in the analysis of *Rpc*, *RSm*, and *Rc* (peak count, mean width of profile elements, and mean height of profile elements, respectively). Seen in Fig. 4, as α decreases, *Rpc* decreases while *RSm* and *Rc* increase, suggesting that the number of peaks decrease but their overall size increases. Based on this result and the qualitative analysis of the surfaces, these changes are indicative of a shift between surfaces dominated by partially melted powder particles (seen at higher values of α or lower powers) and surfaces dominated by material from the re-solidified melt track (seen at lower values of α or higher powers). This result can also be seen in the SEM images presented in Fig. 2 and the respective values of *Rpc*, *RSm*, and *Rc*.

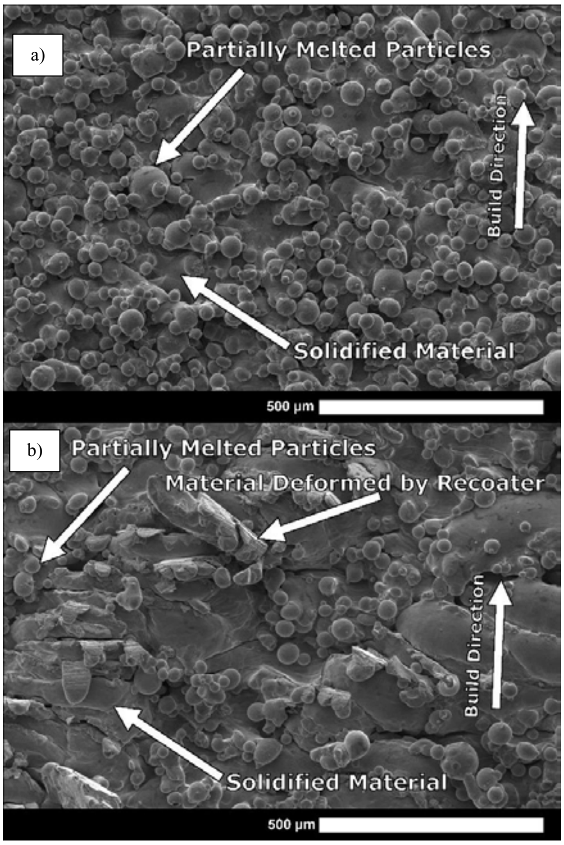


Fig. 2. SEM images of the downward-facing surface of the α=60˚samples built with a) contour parameter set 4 and b) contour parameter set 9.

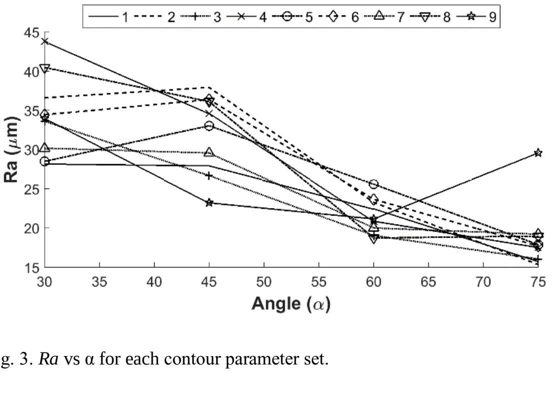


Fig. 3. *Ra* vs α for each contour parameter set.

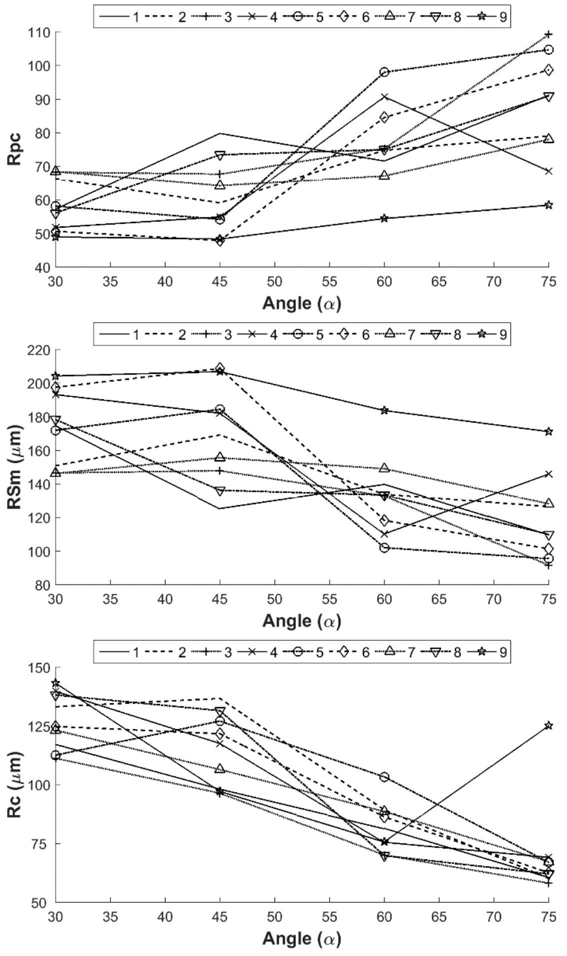


Fig. 4 *Rpc* (top), *RSm* (middle), and *Rc* (bottom) vs. α for each contour parameter set.

5. Conclusions

Analysis of the effect of beam power, beam velocity, and overhang angle has been presented to further the understanding of the relationship between individual surface characteristics and surface roughness parameters. It was found that the analysis of *Rpc*, *RSm*, and *Rc* can indicate a shift between surfaces dominated by partially melted powder particles (seen at higher values of α or lower powers) and surfaces dominated by material from the re-solidified melt track (seen at lower values of α or higher powers).

Analysis of process parameters on *Ra* did not show a distinct correlation, however, and it is suggested that further qualitative analysis of the individual features contributing to surface roughness will help these correlations emerge and will be the focus of future work.

Acknowledgements

The authors would like to thank Dr. Mark Stoudt and Dr. Maureen Williams for their assistance taking SEM images.

References

[1] Liu, X., Chu, P. K., and Ding, C., 2004, “Surface modification of titanium, titanium alloys, and related materials for biomedical applications,” Materials Science and Engineering: R: Reports, **47**(3–4), pp. 49–121. DOI: 10.1016/j.mser.2004.11.001.

[2] Lane, B. M., Moylan, S. P., and Whitenton, E. P., 2015, “Post-Process Machining of Additive Manufactured Stainless Steel,” Proceedings of the 2015 ASPE Spring Topical Meeting: Achieving Precision Tolerances in Additive Manufacturing, ASPE, Raleigh, NC.

[3] Yasa, E., Kruth, J.-P., and Deckers, J., 2011, “Manufacturing by combining Selective Laser Melting and Selective Laser Erosion/laser re-melting,” CIRP Annals - Manufacturing Technology, **60**(1), pp. 263–266. DOI: 10.1016/j.cirp.2011.03.063.

[4] Mumtaz, K. A., and Hopkinson, N., 2010, “Selective Laser Melting of thin wall parts using pulse shaping,” Journal of Materials Processing Technology, **210**(2), pp. 279–287. DOI: 10.1016/j.jmatprotec.2009.09.011.

[5] Pyka, G., Burakowski, A., Kerckhofs, G., Moesen, M., Van Bael, S., Schrooten, J., and Wevers, M., 2012, “Surface modification of Ti6Al4V open porous structures produced by additive manufacturing,” Adv. Eng. Mater., **14**(6), pp. 363–370. DOI: 10.1002/adem.201100344.

[6] 2012, “Measurement Science Roadmap for Metal-Based Additive Manufacturing,” National Institute of Standards and Technology, Gaithersburg, MD.

[7] Kamran Mumtaz, and Neil Hopkinson, 2009, “Top surface and side roughness of Inconel 625 parts processed using selective laser melting,” Rapid Prototyping Journal, **15**(2), pp. 96–103. DOI: 10.1108/13552540910943397.

[8] Strano, G., Hao, L., Everson, R. M., and Evans, K. E., 2013, “Surface roughness analysis, modelling and prediction in selective laser melting,” Journal of Materials Processing Technology, **213**(4), pp. 589–597. DOI: 10.1016/j.jmatprotec.2012.11.011.

[9] Diatlov, A., Buchbinder, D., Meiners, W., Wissenbach, K., and Bultmann, J., 2012, “Towards surface topography: Quantification of Selective Laser Melting (SLM) built parts,” Innovative Developments in Virtual and Physical Prototyping: Proceedings of the 5th International Conference on Advanced Research in Virtual and Rapid Prototyping, Taylor and Francis Inc., Leiria, Portugal, pp. 595–602.

[10] Jamshidinia, M., and Kovacevic, R., 2015, “The influence of heat accumulation on the surface roughness in powder-bed additive manufacturing,” Surf. Topogr.: Metrol. Prop., **3**(1), p. 014003. DOI: 10.1088/2051-672X/3/1/014003.

[11] Triantaphyllou, A., Giusca, C. L., Macaulay, G. D., Roerig, F., Hoebel, M., Leach, R. K., Tomita, B., and Milne, K. A., 2015, “Surface texture measurement for additive manufacturing,” Surf. Topogr.: Metrol. Prop., **3**(2), p. 024002. DOI: 10.1088/2051-672X/3/2/024002.

[12] Vandenbroucke, B., and Kruth, J.-P., 2007, “Selective laser melting of biocompatible metals for rapid manufacturing of medical parts,” Rapid Prototyping Journal, **13**(4), pp. 196–203.

[13] Taylor, J. S., 2015, “Physical processes linking input parameters and surface morphology in additive manufacturing,” Proceedings of the 2015 ASPE Spring Topical Meeting: Achieving Precision Tolerances in Additive Manufacturing, ASPE, Raleigh, NC, pp. 70–71.

[14] “Material data sheet - EOS StainlessSteel GP1” [Online]. Available: https://scrivito-public-cdn.s3-eu-west-1.amazonaws.com/eos/public/5f84f5d2c88ac900/05fb1582834a38c85ef6dd859733a230/EOS_StainlessSteel-GP1_en.pdf. [Accessed: 07-Dec-2015].

[15] Kleszczynski, S., Ladewig, A., Friedberger, K., zur Jacobsmühlen, J., Merhof, D., and Witt, G., “Position Dependency of Surface Roughness in Parts from Laser Beam Melting Systems.”

[16] Leach, R. K., ed., 2010, Fundamental Principles of Engineering Nanometrology, William Andrew Publishing, Oxford.

[17] ISO 4287:1997, 1997, Geometrical Product Specifications (GPS) – Surface texture: Profile method – Terms, definitions and surface texture parameters, ISO, Geneva.

[18] Petzing, J., Coupland, J., Leach, R. K., 2010, “The Measurement of Rough Surface Topography using Coherence Scanning Interferometry”, National Physical Laboratory Good practice guide No. 116, Teddington, UK.

[19] Yasa, E., Deckers, J., Craeghs, T., Badrossamay, M., and Kruth, J.-P., 2009, “Investigation on occurrence of elevated edges in selective laser melting,” International Solid Freeform Fabrication Symposium, Austin, TX, USA, pp. 673–85.

[20] Yadroitsev, I., and Smurov, I., 2011, “Surface Morphology in Selective Laser Melting of Metal Powders,” Physics Procedia, **12, Part A**, pp. 264–270. DOI: 10.1016/j.phpro.2011.03.034.

Fox, Jason; Moylan, Shawn; Lane, Brandon.
“Effect of process parameters on the surface roughness of overhanging structures in laser powder bed fusion additive manufacturing.”
Paper presented at the Procedia CIRP, Charlotte, NC, Jun 8-Jun 10, 2016.

PRELIMINARY STUDY TOWARD SURFACE TEXTURE AS A PROCESS SIGNATURE IN LASER POWDER BED FUSION ADDITIVE MANUFACTURING

Jason C. Fox[1], Shawn P. Moylan[1], and Brandon M. Lane[1]
[1]Intelligent Systems Division
National Institute of Standards and Technology
Gaithersburg, MD 20899

ABSTRACT

Additive manufacturing (AM) allows for highly complex designs that cannot be achieved through subtractive or formative manufacturing techniques. A limiting factor of AM, however, is the as-built surface quality. Additionally, there is limited knowledge on how specific surface features or defects translate to measured surface parameters. If a strong quantitative understanding of the relationships between the processes that cause specific surface features and the measured surface parameters can be developed, then surface texture has the potential to be developed as a process signature. Vertical and upward-facing surfaces of varying angles and process parameters were built and analyzed. Analysis of *Ra* was found to provide little information on the specific features that make up the surface texture. *RSm* and *Rc*, however, can indicate a shift between surfaces dominated by partially melted powder particles and ones dominated by material from the re-solidified melt track, which was also seen for downward-facing surfaces in prior work. The correlations presented are a step toward developing surface texture as a process signature for AM.

INTRODUCTION

Additive manufacturing (AM) has emerged as a key technology for production applications [1]. Laser powder bed fusion (L-PBF), a subset of AM, in particular has generated a great deal of interest. This is due to the fine focusing optics, layer thicknesses of 20 µm to 100 µm, and the powers and velocities over which the system operates allows for fine detail compared to other AM technologies [2].

Despite the advantages of AM, however, a limiting factor affecting widespread adoption is the as-built surface topography of finished parts. Methods exist to process surfaces *in situ* [3,4] or *ex situ* [5,6], but are limited, especially as design complexity increases [7]. Thus, improvements in the as-built surface texture has been cited as a key need [8].

Optimization of surface roughness has been the focus of several studies in AM research. Craeghs *et al.* used optical sensors to control melting, resulting in a reduction in top and overhanging surface roughness [9]. Diatlov *et al.* performed a spectral analysis of the arithmetical mean roughness (*Ra*) for a wide range of surface slopes, finding a potential to determine surface characteristics [10]. Work by Abd-Elghany and Bourell investigated the effect of layer thickness on top and side surface roughness, finding that thick layers lead to increased surface roughness due to a tendency of the particles to form voids once removed during post processing [11]. Jamshidinia and Kovacevic found that an increase in surface roughness can occur due to increased heat accumulation causing an increase in partially melted powder particle attachment [12].

There is a wide range of mechanisms that contribute to the roughness of an AM surface, which include the process input parameters as well as the complex physical processes that occur during melting and solidification of the metal powder [13]. For example, Kleszczynski *et al.* found that there is a positional dependency on surface roughness [14], a factor commonly overlooked by the research community. Additionally, the majority of research cites *Ra* when determining surface roughness; however, this parameter tells us very little about the makeup of the surface. Some research has investigated additional parameters. For example, Triantaphyllou *et al.* found that the area skewness (*Ssk)* can be used to differentiate between upward- and downward-facing surfaces [15]. However, if surface texture is to be used as a process signature a strong quantitative understanding of the relationship

Fox, Jason; Moylan, Shawn; Lane, Brandon.
"Preliminary Study Toward Surface Texture as a Process Signature in Laser Powder Bed Fusion Additive Manufacturing."
Paper presented at the 2016 ASPE Summer Topical Meeting: Dimensional Accuracy and Surface
Finish in Additive Manufacturing, Raleigh, NC, Jun 27-Jun 30, 2016.

between the mechanisms that contribute to surface texture and measured surface parameters, including and not limited to *Ra*, must be investigated and understood.

Related work by the authors has shown the potential of using existing parameters beyond *Ra* to better understand the characteristics of a surface for downward-facing surfaces [16]. In this work, upward-facing and vertical surfaces of the parallelepipeds are analyzed. Qualitative and quantitative analyses show that relationships seen in the mean spacing of profile irregularities (*RSm*) and the mean height of the profile elements (*Rc*) of downward-facing surfaces can also be seen in the vertical and upward-facing surfaces. These correlations point toward a direction for further research into relating surface finish metrics with the physics of the laser powder bed fusion process and the development of surface texture as a process signature.

EXPERIMENTAL PROCEDURE

The experiments focus on test parts that were built on a commercially available L-PBF system. The parts were designed as symmetrical parallelepipeds, having two parallel, vertical parallelogram faces; two rectangular faces; and two square faces. The acute angle of the parallelogram was varied, resulting in test parts with inclined/overhang angles (α) of 30˚, 45˚, 60˚, and 75˚ as measured from the build plane. Figure 1 illustrates the test part with α=60˚.

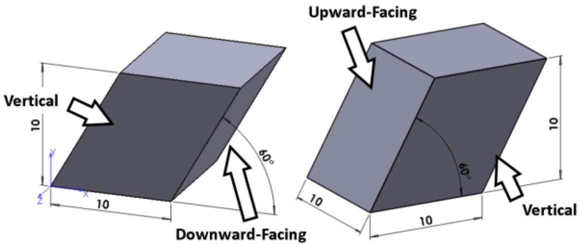


FIGURE 1. Model parallelepiped for surface characterization, where α=60°. Dimensions are in millimeters. Build direction is positive z.

The test parts were built on the EOS M270[1] system at the National Institute of Standards and Technology (NIST). All parts were fabricated in the same build. Stainless steel powder (EOS GP1, which is chemically equivalent to U.S. classification 17-4 stainless steel) reclaimed from several previous builds was used. The powder was screened through an 80 µm sieve before the build. Since it is likely that the condition of the feedstock powder affects the surface texture of the resulting part, powder samples were taken and are currently being analyzed.

Prior work assessed the effect of process parameters on surface characteristics for downward-facing surfaces [16]. In that work, contour parameters with varying laser beam power and travel velocity were chosen in order to cover a wide range of the process space. It was found that two sets of parameters led to highly different surface characteristics. As such, the focus of this work will be on Characterizing the vertical and upward-facing surfaces from the two contour parameters sets shown in TABLE 1.

TABLE 1. Process parameters for experiments. Contour numbers are chosen to match designations from prior work [16].

Contour Number	Power (W)	Velocity (mm/s)	Line Energy – *P/v* (J/m)
4	40	700	57.1
9	195	700	278.6

A total of eight parallelepipeds were analyzed (i.e., two contour parameter sets with four values of α). As such, eight upward-facing surfaces and 16 vertical surfaces were analyzed (since each parallelepiped has two vertical surfaces). Test parts were positioned equidistant from the center of the build platform with the downward-facing surface of the parallelepiped forming a straight line to the center of the laser source. This was done to prevent as many of the positional dependency issues seen by Kleszczynski *et al.* [14] as possible. All surfaces were also at a slight angle (i.e., not parallel) to the recoater blade and that angle varies based on position on the build plate to maintain a constant angle relative to the laser. Additionally, the vertical surfaces are either facing towards the center of the plate (labeled Towards in later figures) or away from the center of the plate (labeled Away).

[1] Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

ANALYSIS METHODS

Surface characterization was performed using a white light interferometer, described in detail in [17], and 10x objective lens. Using white light interferometry to analyze a very rough surface is a challenge due to difficulty in achieving null fringe condition (perfect leveling of the sample surface being measured). Because of this, a diamond-turned aluminum disk was first used to level the sample platform prior to any measurements. Thus, the best leveling possible, assuming that the surface being measured and the surface laying on the platform are parallel, was achieved. This leveling procedure was performed before each measurement session to maintain a consistent leveling for each sample and prevent deviations due to errors caused by the leveling of the samples.

Seven images with 20 percent overlap were taken along each surface (perpendicular to the layers) and stitched together to create an approximately 5 mm long measurement. This created a large enough measurement of the sample surface to properly perform digital Gaussian filtering based on the ISO 4287 standard [18]. The values presented used a bandpass digital Gaussian filter with a short cut-off length of 25 µm and a long cut-off length of 0.8 mm. The filtering process results in an evaluation length equal to five long cut-off lengths, or 4 mm. These filters are defined by ISO 4287 and represent a common practice in AM surface roughness research [19].

Qualitative analysis using scanning electron microscopy was performed on selected surfaces.

RESULTS

Qualitative Analysis

Scanning electron microscope (SEM) images for two vertical surfaces can be seen in FIGURE 2. FIGURE 2a) shows a vertical surface built with set 4. In this image, the surface is dominated by partially melted powder particles, but the re-solidified material from the melt track as well as gaps in the melt surface can be seen.

FIGURE 2b) shows a vertical surface built with set 9. In this image, fewer partially melted particles are present and the surface is dominated by the re-solidified material from the melt track. Additionally, this combination of power and velocity led to material that was damaged by the recoater blade on the downward-facing surface [16]. Similar damage can also be seen in this figure. A key difference between the vertical surface and the downward-facing surface, however, is the nature of the damaged material. These surfaces have a different orientation relative to the recoater blade because they form 90° angle when viewed from above. As such, the damaged material is scraped into the part from the vertical surface and out of the part from the downward-facing surface.

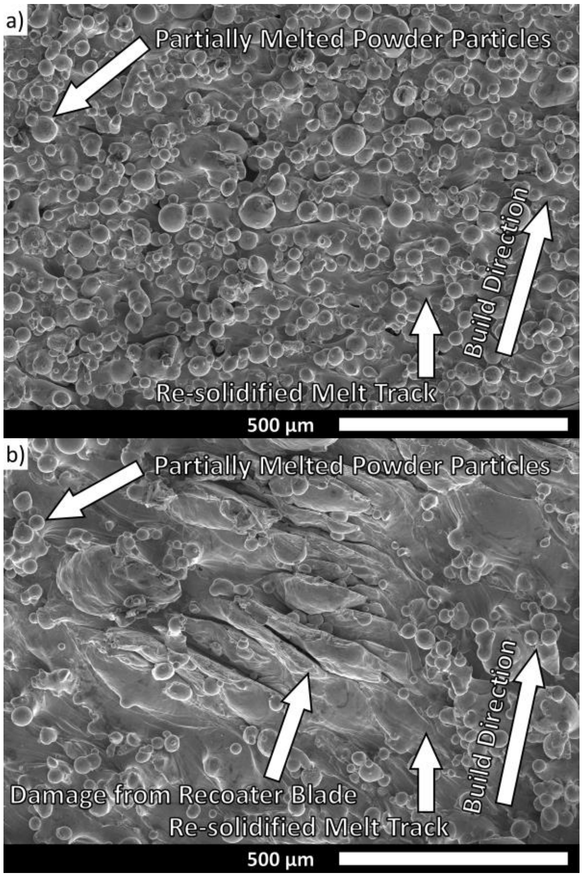


FIGURE 2. Vertical surfaces built with a) set 4 and b) set 9.

SEM images for two upward-facing surfaces can be seen in FIGURE 3. FIGURE 3a) shows the upward-facing surface built with set 4. Similar to the vertical surface with the same set, this surface is dominated by partially melted powder particles but the re-solidified material from the melt track as well as gaps in the melt surface can be seen.

FIGURE 3b) shows the upward-facing surface built with set 9. This surface is dominated by the re-solidified material from the melt track with very few partially melted powder particles. There is no deformation of material that was seen in the vertical and downward-facing surfaces. Additionally, there is little evidence of the layers or of any stair-stepping phenomenon commonly associated with AM.

It is interesting to note that vertical, upward-facing, and downward-facing surfaces built with set 4 are all very similar qualitatively. The selection of this parameter set for the contours would make sense for a manufacturer if having a consistent exterior surface, regardless of position or orientation, is the desirable outcome.

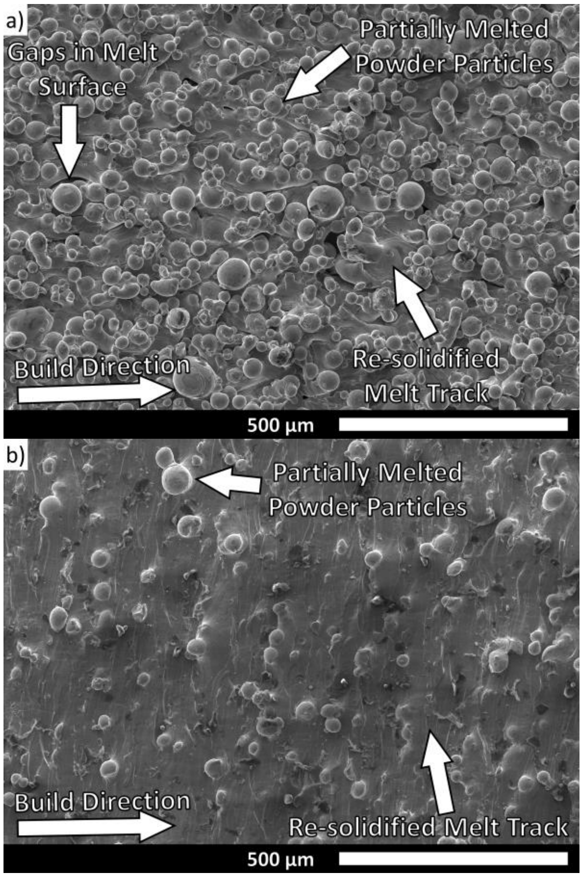


FIGURE 3. Upward-facing surfaces for α=60° built with a) set 4 and b) set 9.

Quantitative Analysis

Vertical Surface Analysis

Analysis of *Ra* for the vertical surfaces can be seen in FIGURE 4. As mentioned previously, these parallelepipeds were built such that the downward-facing surface forms a straight line to the center of the plate. Therefore, the vertical surfaces are either facing towards the center of the plate (labeled Towards) or away from the center of the plate (labeled Away).

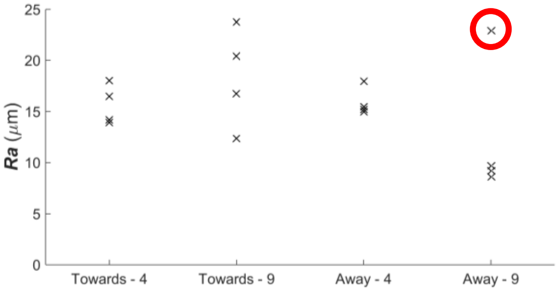


FIGURE 4. Ra vs orientation relative to the center of the build platform and contour parameter set for the vertical surfaces. Outlier described in text is highlighted by a red circle.

FIGURE 4 shows that it is difficult to develop a physical interpretation of the surface through *Ra* alone. An interesting observation, however, is that the high value outlier for the Vertical Away surface built with set 9 (highlighted by the red circle) could be due to the orientation relative to the recoater blade. Three of the vertical surfaces facing away from the center of the plate and built with parameter set 9 were oriented such that the recoater blade was going into the surface when spreading powder, while the outlier was oriented such that the recoater blade was coming out of the surface. Thus, the increase in surface roughness could be due to damaged material protruding from the surface and additional qualitative analysis is required to confirm.

Analysis of *Rc* and *RSm* for the vertical surfaces can be seen in FIGURE 5. Little variation can be seen in *Rc* and *RSm* for the parts built with set 4. For set 9, there is an increase in *RSm* when compared to set 4, which is expected from SEM images as the surface for set 9 is dominated less by partially melted powder particles and more by the re-solidified material from the melt track.

Another interesting finding is the difference in *Rc* for set 9 depending on whether the surface is facing towards or away from the center of the plate. This suggests that there is also a positional dependence in the *Rc* parameter, similar to what was seen by Kleszczynski *et al.* [14], but more qualitative analysis of the surfaces is required to determine the cause of this change.

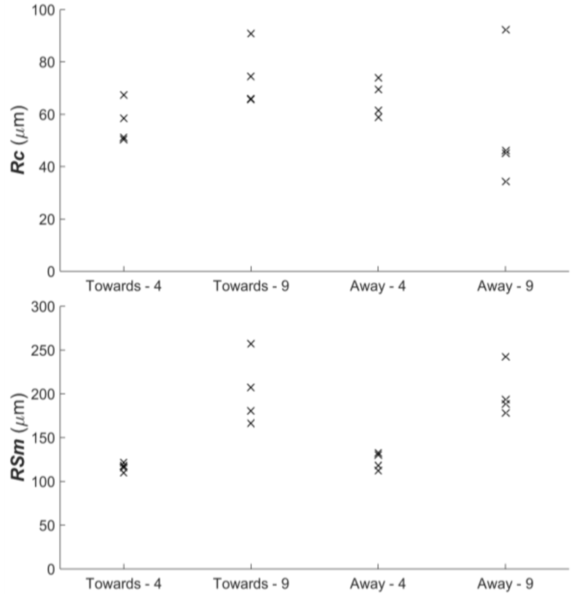


FIGURE 5. Rc and RSm for the vertical surfaces.

Upward-Facing Surface Analysis

Analysis of *Ra* for the upward-facing surfaces as well as the downward-facing surfaces from prior work is presented in FIGURE 6 [16]. As was seen in the prior work, it can be difficult to discern differences in *Ra* from process parameters for the downward-facing surfaces. The upward-facing surfaces, however, exhibit a noticeable difference in *Ra*. Additionally, *Ra* for the upward-facing surfaces built with set 9 decreases as α decreases. This is likely due to the extremely small number of partially melted powder particles seen in SEM images, causing *Ra* to be dependent almost entirely on the re-solidified melt track.

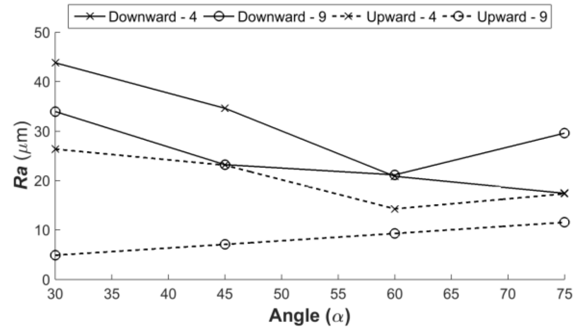


FIGURE 6. Ra vs angle for downward- [16] and upward-facing surfaces.

Analysis of *Rc* and *RSm* for the upward-facing surfaces as well as the downward-facing surfaces from prior work can be seen in FIGURE 7 [16]. As expected, *Rc* decreases and *RSm* increases as we move from surfaces dominated by partially melted powder particles to ones dominated by the re-solidified melt track.

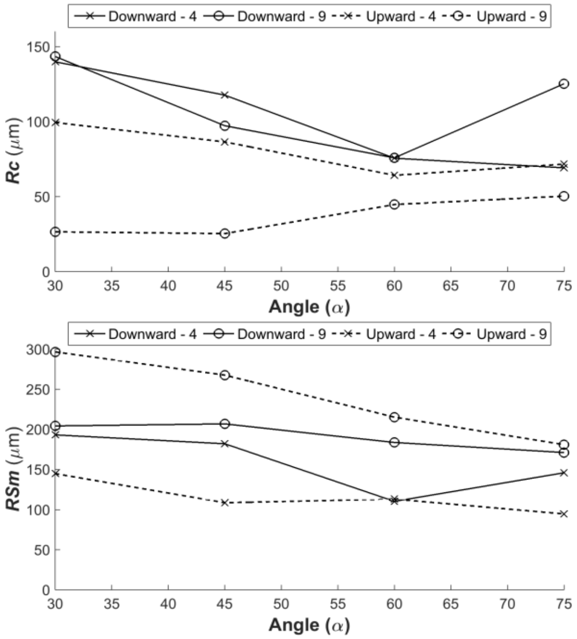


FIGURE 7. Rc and RSm vs angle for downward- [16] and upward-facing surfaces.

CONCLUSIONS

Analysis of upward-facing surfaces of 30°, 45°, 60°, and 75° relative to the build platform and vertical surfaces (90° relative to the build platform) was performed qualitatively by SEM and quantitatively by white light interferometry. Samples were built with two power and velocity combinations, which were found by prior work to create drastic changes in the surface features for downward-facing surfaces [16]. As with the downward-facing surfaces, *Ra* was shown to provide little insight into characteristics of the vertical and upward-facing surface. *Rc* and *RSm* for the vertical and upward-facing surfaces, however, showed similar correlations to the downward-facing surfaces where *Rc* increases and *RSm* decreases as surfaces change from being dominated by the re-solidified melt track to those dominated by the partially melted powder particles. While additional experiments and analysis are required to match specific surface features with the physical process of L-PBF, these correlations provide insight into the use of surface texture as a process signature.

ACKNOWLEGEMENTS

The authors would like to thank Dr. Mark Stoudt and Dr. Maureen Williams of NIST for their assistance with the SEM analyses.

REFERENCES

[1] Taminger KM, Hafley RA. Electron beam freeform fabrication for cost effective near-net shape manufacturing. NATO/RTO AVT-139 Specialists' Meeting on Cost Effective Manufacture via Net Shape Processing, vol. AVT-139, Amsterdam, The Netherlands: 2006, p. 9–25.

[2] Yadroitsev I. Selective laser melting: direct manufacturing of 3D-objects by selective laser melting of metal powders. Saarbrücken: Lambert Acad. Publ; 2009.

[3] Yasa E, Kruth J-P, Deckers J. Manufacturing by combining Selective Laser Melting and Selective Laser Erosion/laser re-melting. CIRP Annals - Manufacturing Technology 2011;60:263–6. doi:10.1016/j.cirp.2011.03.063.

[4] Mumtaz KA, Hopkinson N. Selective Laser Melting of thin wall parts using pulse shaping. Journal of Materials Processing Technology 2010;210:279–87. doi:10.1016/j.jmatprotec.2009.09.011.

[5] Liu X, Chu PK, Ding C. Surface modification of titanium, titanium alloys, and related materials for biomedical applications. Materials Science and Engineering: R: Reports 2004;47:49–121. doi:10.1016/j.mser.2004.11.001.

[6] Lane BM, Moylan SP, Whitenton EP. Post-Process Machining of Additive Manufactured Stainless Steel. Proceedings of the 2015 ASPE Spring Topical Meeting: Achieving Precision Tolerances in Additive Manufacturing, Raleigh, NC: ASPE; 2015.

[7] Pyka G, Burakowski A, Kerckhofs G, Moesen M, Van Bael S, Schrooten J, et al. Surface modification of Ti6Al4V open porous structures produced by additive manufacturing. Advanced Engineering Materials 2012;14:363–70. doi:10.1002/adem.201100344.

[8] Measurement Science Roadmap for Metal-Based Additive Manufacturing, Gaithersburg, MD: NIST; 2012.

[9] Craeghs T, Bechmann F, Berumen S, Kruth J-P. Feedback control of Layerwise Laser Melting using optical sensors. Physics Procedia 2010;5, Part B:505–14. doi:10.1016/j.phpro.2010.08.078.

[10] Diatlov A, Buchbinder D, Meiners W, Wissenbach K, Bultmann J. Towards surface topography: Quantification of Selective Laser Melting (SLM) built parts. Innovative Developments in Virtual and Physical Prototyping: Proceedings of the 5th International Conference on Advanced Research in Virtual and Rapid Prototyping, Leiria, Portugal: 2012, p. 595–602.

[11] Abd-Elghany, K, Bourell, DL. Property evaluation of 304L stainless steel fabricated by selective laser melting. Rapid Prototyping Journal 2012;18:420–8. doi:10.1108/13552541211250418.

[12] Jamshidinia M, Kovacevic R. The influence of heat accumulation on the surface roughness in powder-bed additive manufacturing. Surf Topogr: Metrol Prop 2015;3:14003. doi:10.1088/2051-672X/3/1/014003.

[13] Taylor JS. Physical processes linking input parameters and surface morphology in additive manufacturing. 2015 ASPE Spring Topical Meeting: Achieving Precision Tolerances in Additive Manufacturing, Raleigh, NC: ASPE; 2015, p. 70–1.

[14] Kleszczynski S, Ladewig A, Friedberger K, zur Jacobsmühlen J, Merhof D, Witt G. Position Dependency of Surface Roughness in Parts from Laser Beam Melting Systems. Solid Freeform Fabrication Symposium, Austin, TX: 2015.

[15] Triantaphyllou A, Giusca CL, Macaulay GD, Roerig F, Hoebel M, Leach RK, et al. Surface texture measurement for additive manufacturing. Surf Topogr: Metrol Prop 2015;3:24002. doi:10.1088/2051-672X/3/2/024002.

[16] Fox JC, Moylan SP, Lane BM. Effect of process parameters on the surface roughness of overhanging structures in laser powder bed fusion additive manufacturing. Procedia CIRP, Charlotte, NC: 2016. doi:10.1016/j.procir.2016.02.347.

[17] Leach RK, editor. Fundamental Principles of Engineering Nanometrology. Oxford: William Andrew Publishing; 2010.

[18] ISO 4287:1997. Geometrical Product Specifications (GPS) – Surface texture: Profile method – Terms, definitions and surface texture parameters. ISO, Geneva 1997.

[19] Petzing J, Coupland J, Leach RK. The Measurement of Rough Surface Topography using Coherence Scanning Interferometry. National Physical Laboratory Good Practice Guide No. 116, Teddington, UK: 2010.

Invited Paper

Exploring frustrated magnetism with artificial spin ice

Ian Gilbert*[a] and B. Robert Ilic[a]

[a]Center for Nanoscale Science and Technology, National Institute of Standards and Technology, 100 Bureau Dr., MS6202, Gaithersburg, MD 20899

ABSTRACT

Nanomagnet arrays known as artificial spin ice provide insight into the microscopic details of frustrated magnetism because, unlike natural frustrated magnets, the individual moments can be experimentally resolved and the lattice geometry can be easily tuned. Most studies of artificial spin ice focus on two lattice geometries, the square and the kagome lattices, due to their direct correspondence to natural spin ice materials such as $Dy_2Ti_2O_7$. In this work, we review experiments on these more unusual lattice geometries and introduce a new type of nanomagnet array, artificial spin glass. Artificial spin glass is a two-dimensional array of nanomagnets with random locations and orientations and is designed to elucidate the more complex frustration found in spin glass materials.

Keywords: Artificial spin ice, frustrated magnetism, spin ice, spin glass

1. INTRODUCTION

When the interactions between the microscopic components of a condensed matter system (e.g., the atomic spins in a magnetic material) cannot all simultaneously be satisfied, the system is said to be frustrated. This competition between interactions produces a broad range of interesting phenomena[1]. Examples of geometrically frustrated magnetic materials are the spin ices $Ho_2Ti_2O_7$ and $Dy_2Ti_2O_7$[2]. The pyrochlore crystal lattice of these materials includes a network of corner-sharing tetrahedra with Dy ions located at each tetrahedron corner, and crystal field constrains the rare earth ions' moments to point directly into or out of the tetrahedra. The rare earth spins' ferromagnetic coupling is frustrated in this geometry, because there is no way to place four spins on the four corners of a tetrahedron such that they all point head-to-tail. This geometrical frustration produces a six-fold degenerate "compromise" configuration in which two spins point into and two spins point out of each tetrahedron[3]. The frustration of spin ice causes two particularly interesting effects. First, the degeneracy associated with this two-in, two-out "ice rule" gives spin ice a residual entropy that persists down to the lowest experimentally-accessible temperatures[4]. Second, the elementary excitations of spin ice behave like magnetic monopoles[5]. An excitation occurs wherever the ice rule is broken, and if one considers the spins not as point dipoles but as separate north and south magnetic poles, the adjacent tetrahedra (three-in, one-out or vice versa) will have a net magnetic charge. These monopole excitations can move apart by reversing a chain of spins called (again in analogy with magnetic monopoles) a Dirac string.

Artificial spin ice was developed as a mesoscopic analog to spin ice systems such as $Dy_2Ti_2O_7$[6]. Elongated islands a few hundred nanometers long and made from a ferromagnetic material such as permalloy ($Ni_{81}Fe_{19}$) are fabricated in frustrated lattices to model spin ice. The islands contain a single ferromagnetic domain that is constrained by the island's shape anisotropy to point along the island's long axis, which makes the island moment behave like a giant Ising spin. Artificial spin ice possesses two advantages over natural spin ice. First, because the samples are fabricated using electron beam lithography, the sample geometry can be easily tuned. The island shape and size can be modified to change the properties of the moments, the lattice constant can be tuned over a wide range, and the lattice geometry can be changed at will. Such tailoring of interactions is not possible with natural materials like spin ice. Second, the exact configuration of the individual island moments can be imaged using techniques such as magnetic force microscopy (MFM), something that is not possible for atomic spins in bulk crystals. The first experiments on artificial spin ice demonstrated that when nanomagnets were arranged on a frustrated square lattice (an example of which is shown in Figure 1), an ice rule analogous to that found in spin ice resulted[6]. The vertices (sites at which several islands converge) of the square lattice exhibited a strong preference for configurations obeying the two-moments-in, two-moments-out ice rule. Further experiments have shown monopole-like excitations similar to those found in spin ice[7,8]. The majority of artificial spin ice investigations have considered the square and kagome lattices. Since these results have been described recently in

Spintronics IX, edited by Henri-Jean Drouhin, Jean-Eric Wegrowe, Manijeh Razeghi, Proc. of SPIE
Vol. 9931, 99311P · © 2016 SPIE · CCC code: 0277-786X/16/$18 · doi: 10.1117/12.2237000

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 09/30/2016 Terms of Use: http://spiedigitallibrary.org/ss/termsofuse.aspx

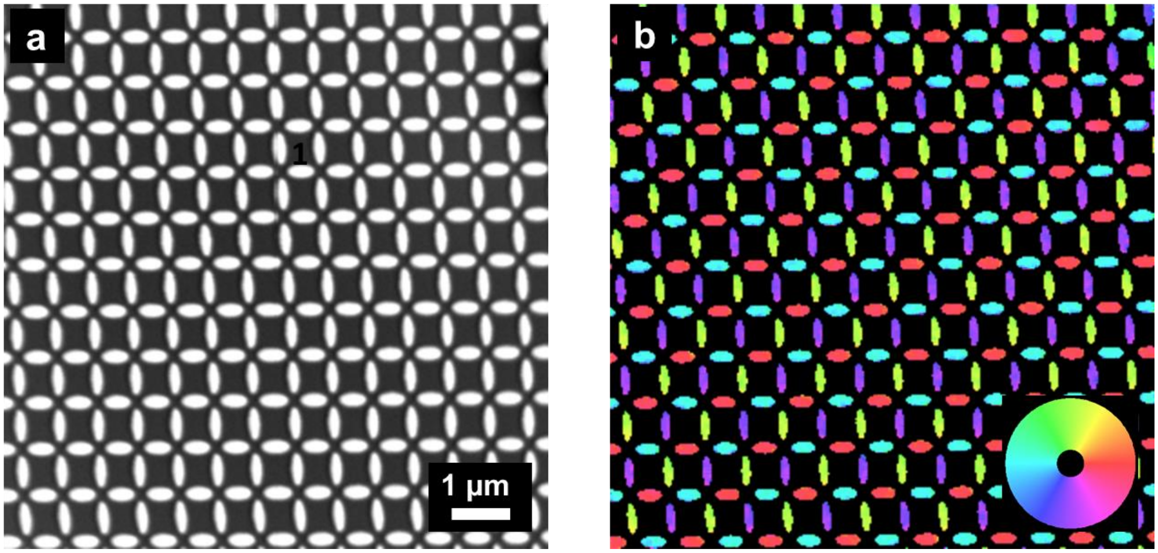


Figure 1. Artificial square spin ice. Panel (a) shows a scanning electron micrograph of a lattice comprised of 470 nm × 170 nm elliptical islands arranged on a square array with lattice constant 700 nm. Panel (b) shows an image taken with scanning electron microscopy with polarization analysis (SEMPA), which reveals the direction of each island's magnetization. The magnetization direction is color coded according to the color wheel inset in the lower right corner, and nonmagnetic areas are black. This particular sample is in its ground state, which is an ordered arrangement of island moments with two moments pointing into and two out of each vertex (the sites where four islands come together in the shape of a plus sign).

several excellent review articles[9,10], here we will focus on reviewing other, more novel lattice geometries, describing both completed experiments and further proposals.

2. TUNING GEOMETRICAL FRUSTRATION

Many of the early studies of new lattice geometries utilized the triangular lattice in various forms. Several possibilities are shown in Figure 2. The first consists of collinear nanomagnets placed on the points of a triangular Bravais lattice, as shown in Figure 2a. Ising spins with equal nearest-neighbor antiferromagnet interactions on a lattice comprised of equilateral triangles is one of the first (and simplest) examples of geometrical frustration[11]. The anisotropy of the dipolar interactions of the in-plane-magnetized islands reduces the degree of frustration and permits several types of order to develop[12], depending on the relative size of the two lattice constants (labeled *x* and *d* in Figure 2a). A detailed analysis of the correlations between island moments in the triangular lattice revealed that in some cases the sign of the correlation between two islands was opposite what one would expect based on the sign of the dipolar interaction[13]. This was attributed to indirect interactions between the two islands mediated by other, neighboring islands, analogous to the Ornstein-Zernike theory used to describe the structure of liquids. Another possible arrangement of islands is to place the long islands between the points of a triangular Bravais lattice, with the island long axes parallel to the lattice vectors (Figure 2b). This scenario was considered from a theoretical perspective by Mól and coworkers, who noted that such a system has several different types of magnetically-charged excitations (e.g., six-out, five-out, one-in, etc.). Furthermore, some of these magnetically-charged excitations are lower in energy than uncharged excitations, and the tension (energy per unit length) of strings of flipped moments connecting excitations can have a wide range of values. This artificial triangular spin ice has not yet been studied experimentally. The third possible triangular lattice arrangement (Figure 2c) is to place islands magnetized normal to the lattice on the points of a triangular lattice[15,16] (or the related hexagonal and kagome lattices[17]). These arrays of perpendicularly-magnetized islands could be of significant interest in the context of frustrated magnetism because the dipolar interaction between two islands depends on distance only, and not on the angle between the islands' long axes, as is the case for in-plane magnetized islands.

Frustrated nanomagnet arrays are not restricted to periodic lattices. A number of works have examined artificial quasicrystals, in which (connected) permalloy bars are arranged along the edges of Penrose[18,19] or Ammann tilings[20].

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 09/30/2016 Terms of Use: http://spiedigitallibrary.org/ss/termsofuse.aspx

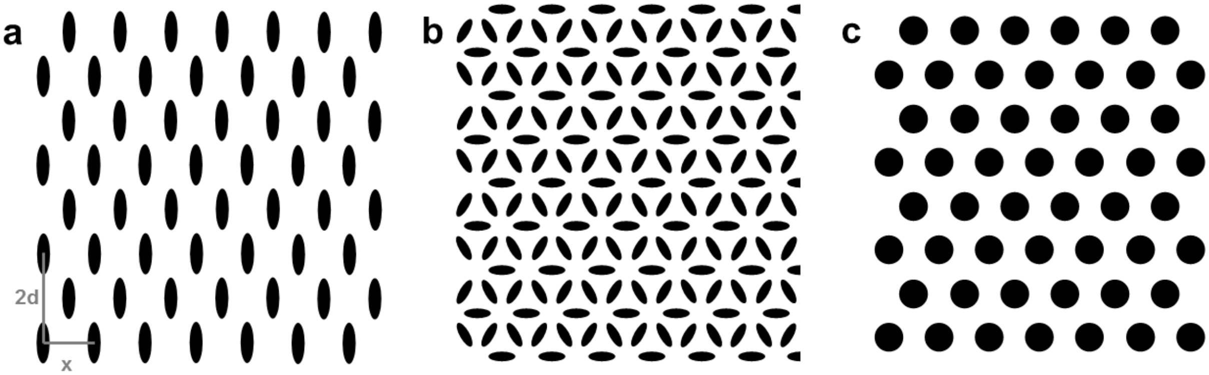


Figure 2. Various geometries for triangular artificial spin ice. Several early papers considered collinear (in-plane magnetized) islands arranged on a planar triangular lattice (a). Mól et al. used the same type of islands, but placed them along the edges of a triangular lattice (b). Finally, several papers have used circular islands made from materials with out-of-plane magnetization (e.g., Pt/Co multilayers). Arranging these islands on a triangular lattice yields a frustrated triangular-lattice antiferromagnetic system (c).

Like quasicrystal materials, these two-dimensional artificial quasicrystals have long-range order but lack translational symmetry, and like artificial spin ice, the vertices in artificial quasicrystals generally obey an ice rule dictating the number of moments pointing into or out of a vertex, and they have a large number of low-energy configurations produced by frustration[19]. The connected quasicrystal lattices differ from artificial spin ice comprised of disconnected islands, however, in that short-range exchange interactions also contribute to the energy hierarchy of vertex configurations, and magnetization reversal may occur via domain wall propagation.

3. VERTEX FRUSTRATION

In 2013, Morrison and coworkers introduced the concept of *vertex frustration* in artificial spin ice[21], examples of which is shown in Figure 3. In a non-vertex-frustrated lattice, the nanomagnets in each vertex (clusters of several converging islands) can arrange their moments such that the magnetostatic energy of the vertex is minimized. But in a vertex-frustrated array, interactions with the neighboring portions of the lattice prevent some of the vertices from achieving the lowest-energy state. Vertex frustration is similar to ordinary geometrical frustration because, in both cases, constraints imposed by the lattice geometry frustrate the system and lead to a degeneracy of low energy states. Vertex frustration differs from ordinary geometrical frustration because the basic units being frustrated are the vertices rather than the individual island moments. Using vertex frustration, one can design a large number of complex lattice structures that can be specifically tuned to exhibit a physical phenomenon of interest. The original theory paper of Morrison *et al.* described the structure of half a dozen vertex-frustrated lattices and predicted their ground states[21], only a few have yet been experimentally studied.

The vertex-frustrated lattice which has received the most scrutiny is the shakti lattice[21-23]. Like many vertex-frustrated lattices, the shakti lattice is a modification of the square lattice, in this case with one quarter of the islands removed. The lattice, shown in Figure 3a, contains both three- and four-island vertices, and the lattice geometry prevents all of the vertices from reaching their ground state configurations. By considering the relative energy cost of the various possible defects, one can show that the best possible energy minimization involves placing half of the three-island vertices in defect configurations. This means that each square plaquette (one plaquette is indicated in light blue in Figure 3a) of the lattice will contain two ground-state vertices and two excited vertices, and there will be six ways of arranging the excited vertices, all with the same energy. This degeneracy in vertex arrangements mimics the original frustration of natural spin ice, something that two-dimensional artificial square spin ice is unable to do because of geometry constraints and the anisotropy of the dipolar interaction. Gilbert *et al.* were able to directly observe this “ice rule for vertices” using magnetic force microscopy to image a thermally annealed sample of shakti artificial spin ice[22]. The three-island vertices

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 09/30/2016 Terms of Use: http://spiedigitallibrary.org/ss/termsofuse.aspx

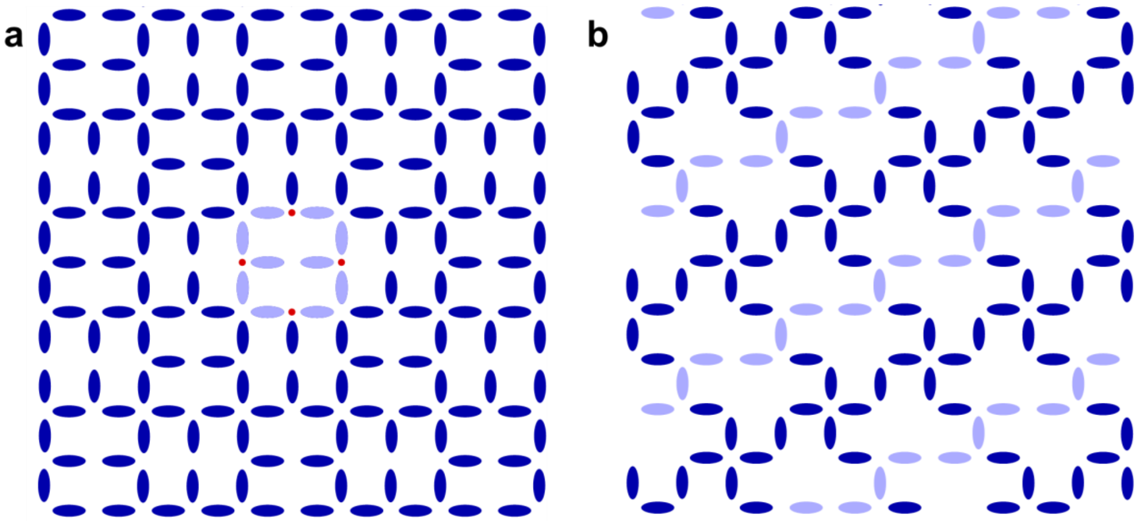


Figure 3. Examples of vertex frustration. (a) The structure of the shakti lattice. One of the plaquettes comprising the lattice is indicated in light blue, and the four three-island vertices of this plaquette are marked with red dots. In the ground state, half of the three island vertices are forced into defect configurations, so two of these four sites will contain a defect, and there are six possible ways of arranging the two defects on the four sites. (b) The structure of the tetris lattice. The lattice can be decomposed into alternating one-dimensional bands, shown here in light and dark blue. The dark blue bands are not vertex-frustrated and take on an ordered configuration, while the light blue bands are vertex-frustrated, remaining disordered and also (relative to the dark blue bands) susceptible to thermal fluctuations.

also possess a magnetic charge and were observed to organize themselves into antiferromagnetically-ordered domains similar to those observed in thermally annealed artificial kagome spin ice[24]. They also effectively screen the occasional monopole-like defects observed on four-island vertices. The shakti lattice is also predicted to develop an emergent sliding symmetry within the charge-ordered phase[23], but this has not yet been experimentally observed.

The tetris lattice (Figure 3b) is another vertex-frustrated lattice that has been experimentally fabricated and imaged[21,25]. This lattice contains alternating bands of vertex-frustrated (light blue) and non-vertex-frustrated (dark blue) bands. After thermalization, the non-frustrated bands exhibit long-range ordering, while the vertex-frustrated bands are disordered. Correlations between moments in the disordered vertex-frustrated bands match those predicted by a thermal one-dimensional Ising model, so in this case, vertex frustration leads to dimensionality reduction within a two-dimensional lattice[24]. The vertex frustration of the tetris lattice also affects the dynamics: the ordered bands freeze into a single well-defined ground state at a temperature at which the vertex-frustrated bands are still fluctuating among their many low-energy configurations.

4. ARTIFICIAL SPIN GLASS

All of the types of artificial spin ice described up to this point consist of regular lattices that possess translational symmetry or, in the case of the artificial quasicrystals, at least some type of long range structural order and rotational symmetry. Frustrated magnetism is not, however, limited to geometrically frustrated regular lattices. Spin glasses, for instance, are alloys in which magnetic ions are distributed randomly throughout a nonmagnetic host material[26,27]. The interactions between these isolated moments vary in strength and sign and can frustrate one another. Here we describe some preliminary measurements of artificial spin glass, a nanomagnet array similar to artificial spin ice but designed to model the random frustration of spin glasses.

The islands comprising the arrays are ellipses with major and minor axes of 470 nm and 170 nm (design values), respectively. The arrays were generated by placing islands within a 60 µm × 60 µm square with x and y coordinates and orientations drawn from a random uniform distribution. An island location was rejected if a 590 nm diameter circle centered on the ellipse would overlap with another such circle centered on any of the neighboring ellipses. Arrays with

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 09/30/2016 Terms of Use: http://spiedigitallibrary.org/ss/termsofuse.aspx

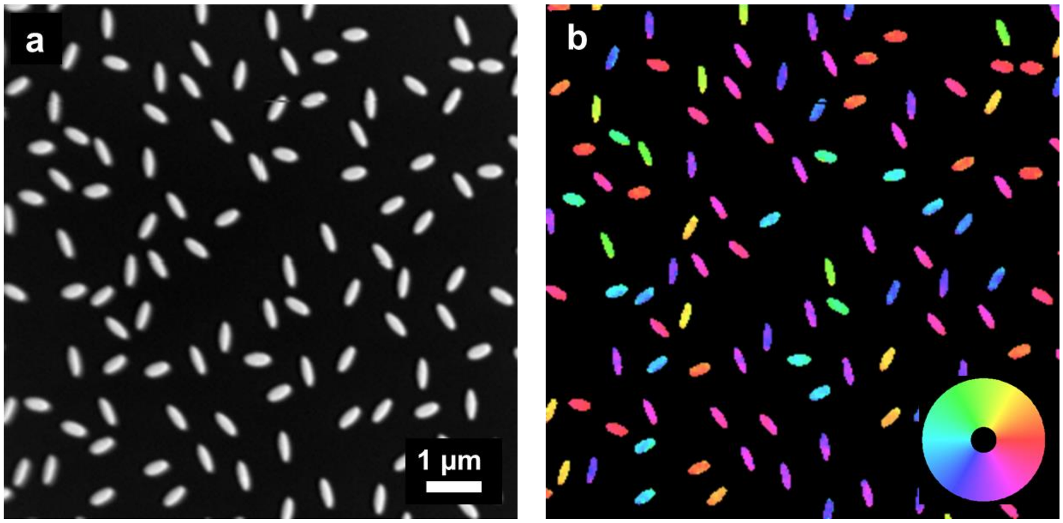


Figure 4. Artificial spin glass. A scanning electron micrograph of the randomly located and oriented islands is shown in (a) for a sample with 7500 islands arranged in a 60 µm × 60 µm area. Panel (b) depicts the corresponding SEMPA image, which reveals island moments pointing in random directions with no type of order present.

2500, 5000, and 7500 islands were fabricated using a standard electron beam lithography process with a bilayer resist stack that is described elsewhere[24]. An artificial square spin ice array with 700 nm lattice constant was fabricated on the same sample to verify thermalization of the island moments. A ≈6 nm $Ni_{80}Fe_{15}Mo_5$ film was deposited on a doped silicon substrate at ≈0.05 nm/s via electron beam evaporation, with a ≈2 nm Pt capping layer to prevent oxidation, followed by liftoff. The configuration of the island moments was measured using scanning electron microscopy with polarization analysis (SEMPA). The Pt capping layer was removed with in situ Ar^+ ion etching, and a few monolayers of Fe were evaporated to increase the magnetic contrast (this Fe film is thin enough to remain paramagnetic on the nonmagnetic regions of the sample while exchange coupling to the island magnetization and increasing the electron polarization measured by SEMPA). The square lattice, which was shown in Figure 1, is in its completely-ordered ground state, indicating that the island moments were able to thermally equilibrate during the thin film deposition[28]. The artificial spin glass array (Figure 4) shows islands magnetized in all directions. The random structure of the lattice precludes the type of spatially-periodic long-range magnetic order found in the square lattice (Figure 1b), though there is a small net magnetic moment for area of the sample shown in Figure 4 ($M_x = 0.05 \pm 0.02$, $M_y = -0.08 \pm 0.02$, where the magnetization is normalized such that M_x (M_y) = 1 if the sample magnetization is saturated in the x (y) direction and the uncertainty represents the standard error calculated from the standard deviation of the distribution of island moment directions). This artificial spin glass sample allows the direct visualization of the random frustration of magnetic moments present in spin glass. Future work on artificial spin glass samples may allow the quantification of frustration as a function of areal density of islands and the exploration of the role of random frustration in determining the system's susceptibility to thermal fluctuations.

5. SUMMARY

Artificial spin ice permits the detailed study of frustration on a microscopic level while providing the ability to tune the interactions between magnetic moments. The geometries described here, such as the various triangular lattices, quasicrystals, and vertex frustrated lattices, provide an interesting way to probe the physics of frustration that complements measurements on the conventional square and kagome artificial spin ices. Even these are not a complete catalog of the possibilities for artificial magnetic materials. Defects such as dislocations can be individually fabricated and measured in artificial spin ice. Drisko and coworkers demonstrated that dislocations in artificial square spin ice nucleated strings of excited vertices that extended either to another dislocation or the array edge[29]. Recently, a modified artificial spin ice lattice designed to allow eight different ordered configurations has been described[30]. The magnetic charges of the vertices in this system should allow information recording, and the states of the individual vertices can be

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 09/30/2016 Terms of Use: http://spiedigitallibrary.org/ss/termsofuse.aspx

modified with the combined effects of an applied magnetic field and a magnetized MFM tip. The possibility of three-dimensional artificial spin ice remains appealing from a theory perspective[31-33], though the challenges of fabricating such a complicated lattice structure have limited its experimental realization[34]. The magnetic moments comprising an array need not even be Ising spins: artificial XY model arrays[34] and an artificial Potts model (even utilizing the magnetocrystalline anisotropy of Fe films[35]) have already been demonstrated. While the direct visualizations of the ice rule and magnetic monopole-like excitations have already been achieved, new lattice geometries promise to provide even more insight into the physics of frustration.

6. ACKNOWLEDGEMENTS

This project was supported by the National Institute of Standards and Technology, Center for Nanoscale Science and Technology under project numbers R13.0004.04 and N09.0017.07 (nanofabrication). I.G. acknowledges support from the National Research Council's Research Associateship Program and thank John Unguris for assistance with SEMPA measurements.

REFERENCES

[1] Moessner, Roderich and Ramirez, Arthur P., "Geometrical frustration," Phys. Today 59(2), 24 (2006).

[2] Castelnovo, C., Moessner, R. and Sondhi, S.L., "Spin ice, fractionalization, and topological order," Annu. Rev. Condens. Matter Phys. 3(1), 35-55 (2012).

[3] Harris, M.J. et al., "Geometrical frustration in the ferromagnetic pyrochlore $Ho_2Ti_2O_7$," Phys. Rev. Lett. 79(13), 2554-2557 (1997).

[4] Ramirez, A.P. et al., "Zero-point entropy in 'spin ice'," Nature 399(6734), 333-335 (1999).

[5] Castelnovo, C., Moessner, R and Sondhi, S.L., "Magnetic monopoles in spin ice," Nature 451(7174), 42-45 (2008).

[6] Wang, R.F. et al., "Artificial 'spin ice' in a geometrically frustrated lattice of nanoscale ferromagnetic islands," Nature 439(7074), 303-306 (2006).

[7] Ladak, S. et al., "Direct observation of magnetic monopole defects in an artificial spin-ice system," Nature Phys. 6(5), 359-363 (2010).

[8] Mengotti, E. et al., "Real-space observation of emergent magnetic monopoles and associated Dirac strings in artificial kagome spin ice," Nature Phys. 7(1), 68-74 (2011).

[9] Heyderman, L.J. and Stamps, R.L., "Artificial ferroic systems: novel functionality from structure, interactions, and dynamics," J. Phys. Condens. Matter 25(36), 363201 (2013).

[10] Nisoli, Cristiano, Moessner, Roderich and Schiffer, Peter, "Colloquium: Artificial spin ice: Designing and imaging magnetic frustration," Rev. Mod. Phys. 85(4), 1473-1490 (2013).

[11] Wannier, G.H., "Antiferromagnetism. The triangular Ising net," Phys. Rev. 79(2), 357-364 (1950).

[12] Ke, Xianglin et al., "Tuning magnetic frustration of nanomagnets in triangular-lattice geometry," Appl. Phys. Lett. 93(25), 252504 (2008).

[13] Zhang, Sheng et al., "Ignoring your neighbors: Moment correlations dominated by indirect or distant interactions in an ordered nanomagnet array," Phys. Rev. Lett. 107(11), 117204 (2011).

[14] Mól, L.A.S., Pereira, A.R. and Moura-Melo, W.A., "Extending spin ice concepts to another geometry: The artificial triangular spin ice," Phys. Rev. B 85, 184410 (2012).

[15] Mengotti, E. et al., "Dipolar energy states in clusters of perpendicular magnetic nanoislands," J. Appl. Phys. 105(11), 113113 (2009).

[16] Fraleigh, Robert D. et al., "Characterization of switching field distributions in Ising-like magnetic arrays," preprint at http://arxiv.org/abs/1606.02770 (2016).

[17] Zhang, Sheng et al., "Perpendicular magnetization and generic realization of the Ising model in artificial spin ice," Phys. Rev. Lett. 109(8), 087201 (2012).

[18] Bhat, V.S. et al., "Controlled magnetic reversal in permalloy films patterned into artificial quasicrystals," Phys. Rev. Lett. 111(7), 077201 (2013).

[19] Farmer, B. et al., "Direct imaging of coexisting ordered and frustrated sublattices in artificial ferromagnetic quasicrystals," Phys. Rev. B 93, 134428 (2016).

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 09/30/2016 Terms of Use: http://spiedigitallibrary.org/ss/termsofuse.aspx

[20] Bhat, V.S. et al., “Ferromagnetic resonance study of eightfold artificial ferromagnetic quasicrystals,” J. Appl. Phys. 115, 17C502 (2014).

[21] Morrison, Muir J., Nelson, Tammie R. and Nisoli, Cristiano, “Unhappy vertices in artificial spin ice: new degeneracies from vertex frustration,” New J. Phys. 15(4), 045009 (2013).

[22] Gilbert, Ian et al., “Emergent ice rule and magnetic charge screening from vertex frustration in artificial spin ice,” Nature Phys. 10, 670-675 (2014).

[23] Chern, Gia-Wei, Morrison, Muir J. and Nisoli, Cristiano, “Degeneracy and criticality from emergent frustration in artificial spin ice,” Phys. Rev. Lett. 111(17), 177201 (2013).

[24] Zhang, S. et al., “Crystallites of magnetic charges in artificial spin ice,” Nature 500, 553-557 (2013).

[25] Gilbert, I. et al., “Emergent reduced dimensionality by vertex frustration in artificial spin ice,” Nature Phys. 12, 162-165 (2016).

[26] Binder, K. and Young, A.P., “Spin glasses: Experimental facts, theoretical concepts, and open questions,” Rev. Mod. Phys. 58(4), 801-976 (1986).

[27] Mydosh, J.A., [Spin Glasses: An Experimental Introduction], Taylor & Francis, London & Washington DC, (1997).

[28] Morgan, J.P. et al., “Thermal ground-state ordering and elementary excitations in artificial magnetic square ice,” Nature Phys. 7(1), 75-79 (2011).

[29] Drisko, Jasper, Marsh, Thomas and Cumings, John, “Topological frustration of artificial spin ice,” preprint at http://arxiv.org/abs/1512.01522.

[30] Wang, Yong-Lei et al., “Rewritable artificial magnetic charge ice,” Science 352(6288) 962-966 (2016).

[31] Möller, G. and Moessner, R., “Artificial square ice and related dipolar nanoarrays,” Phys. Rev. Lett. 96(23), 237202 (2006).

[32] Mól, L.A.S., Moura-Melo, W.A., and Pereira, A.R., “Conditions for free magnetic monopoles in nanoscale square arrays of dipolar spin ice,” Phys. Rev. B 82, 054434 (201).

[33] Chern, Gia-Wei, Reichhardt, Charles and Nisoli, Cristiano, “Realizing three-dimensional artificial spin ice by stacking planar nano-arrays,” Appl. Phys. Lett. 104(1), 013101 (2014).

[34] Mistonov, A.A. et al., “Three-dimensional artificial spin ice in nanostructured Co on an inverse opal-like lattice,” Phys. Rev. B 87, 220408 (2013).

[35] Arnalds, Unnar B. et al., “Thermal transitions in nano-patterned XY-magnets,” Appl. Phys. Lett. 105(4), 042409 (2014).

[36] Louis, D. et al., “Interfaces anisotropy in single crystal V/Fe/V trilayer,” J. Magn. Magn. Mater. 372, 233-235 (2014).

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 09/30/2016 Terms of Use: http://spiedigitallibrary.org/ss/termsofuse.aspx

DYNAMIC CHARACTERIZATION OF IN-PLANE BULK ACOUSTIC RESONATORS USING HIGH-SENSITIVITY OPTICAL REFLECTION MEASUREMENTS

Vikrant J. Gokhale[1, 2] *and Jason J. Gorman*[1]
[1]National Institute of Standards and Technology, Gaithersburg, MD 20899-8212, USA
[2]University of Michigan, Ann Arbor, MI 48109-2122, USA

ABSTRACT

Two experimental techniques for measuring dynamic displacement and strain for in-plane bulk acoustic resonators are presented. These techniques, optical knife-edge and photoelastic measurements, can characterize in-plane high-frequency vibrations with a degree of precision and simplicity that has not been shown previously with MEMS. The measurements are spatially resolved and can be used to reconstruct the vibrational mode shape of the resonator. Experimental results presented here are acquired using both methods on a single crystal silicon bulk acoustic resonator (SiBAR) with a fundamental resonance frequency of ≈ 13.6 MHz.

INTRODUCTION

Capacitive [1] and piezoelectric [2] bulk acoustic resonators (BARs) have received considerable attention over the last decade due to applications in RF timing, filtering, and sensing. Much of the success of these resonators stems from their ability to vibrate in a specific mode with a high mechanical quality factor and hence a sharp spectral linewidth. Contemporary design of micromechanical resonators is heavily reliant on analytical equations and finite element analysis (FEA) of the device, followed by electrical validation. However, the drawback of purely electrical characterization is that it presents only an aggregate signal at the output transduction port of the system (e.g., capacitively induced current). As a result, all-electrical transduction obscures the internal mechanics of the resonator, making it difficult to determine the causes of spurious modes, nonlinearities, and other phenomena. In contrast, optical techniques can provide more detailed and precise characterization of the resonator through spatially and temporally resolved measurement of the absolute device displacement. Laser Doppler vibrometry has been used successfully to measure BARs but typically only for out-of-plane motion [3]. Recently, three-dimensional laser Doppler vibrometry has been demonstrated but at considerable expense and complexity and with limited bandwidth for BARs [4]. Optical knife-edge [5, 6] and photoelastic [7] measurement techniques provide high-sensitivity in-plane motion measurements with simplicity and high bandwidth, as demonstrated by others for surface acoustic waves [7], but have received little attention for BARs, which has motivated the presented research.

DESCRIPTION OF DEVICE & FABRICATION

The devices used in this work are silicon bulk acoustic resonators (SiBAR) that vibrate in their extensional in-plane modes (Fig. 1). The SiBARs are fabricated using standard silicon-on-insulator (SOI) processes. First, metal electrodes are patterned and evaporated using liftoff on an SOI wafer. The device layer of the SOI wafer, which is approximately 10 µm thick, is patterned and etched using deep reactive ion etching (DRIE) to form the transduction gaps and release etch holes. A transduction gap of ≈ 480 nm is achieved using 5X reduction stepper lithography. The DRIE is optimized to provide vertical sidewalls with scallop depths of ≈ 80 nm/cycle and scalloping undercut on the order of ≈ 15 nm. The wafer is diced into individual chips and the mechanical structure is released by etching the 2 µm thick buried oxide layer using hydrofluoric acid vapor.

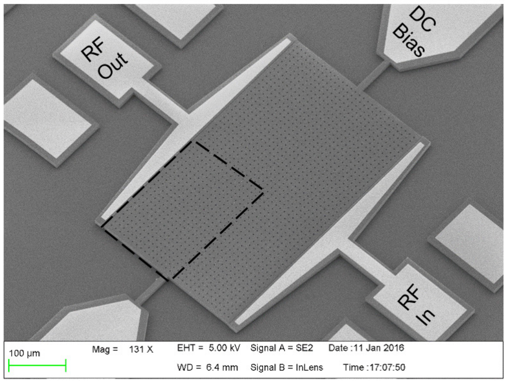


Figure 1: Scanning electron image of a width-extensional single crystal SiBAR with a transduction gap of 480 nm and a measured fundamental resonance frequency of ≈ 13.6 MHz. The resonator width is 300 µm, with an expected resonance frequency of 13.8 MHz. These SiBARs are used as a platform for demonstrating precise dynamic measurements of driven motion and energy dissipation mechanisms. Due to the symmetry of the SiBAR, only one quadrant of the device (boxed) is measured and simulated.

CHARACTERIZATION TECHNIQUES

Electrical Measurements

The released SiBAR was first tested electrically using a vector network analyzer (VNA) and ground-signal-ground (GSG) probes. Standard short-open-load-through (SOLT) calibration is performed prior to acquiring the data seen in Fig. 2. It is observed that the device requires a fairly large DC bias to transduce a measurable resonance, and the signal-to-noise ratio (SNR) is low due to the presence of parasitic feedthrough. The effect of parasitics can be reduced by optimized design, a smaller transduction gap, or electronic signal amplification, but as will be demonstrated in further sections, these improvements are not necessary for optical readout and characterization.

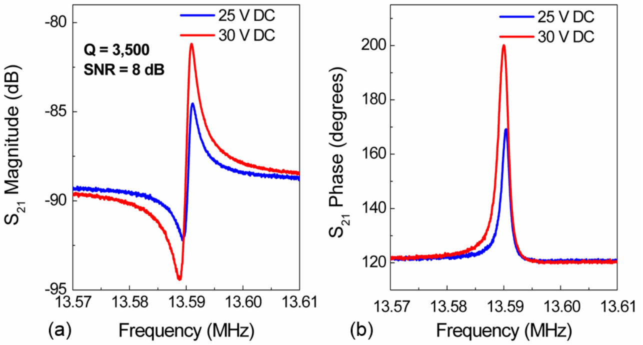


Figure 2: Standard electrical testing of the ≈ 13.6 MHz SiBAR in air, prior to wire-bonding, using GSG probes and a VNA. Magnitude (a) and phase (b) information are shown. Amplification was not used in these tests. No response is seen below ≈ 20 V DC bias, primarily due to the effect of the parasitic feedthrough from the device, bond pads, and handle wafer.

Gokhale, Vikrant; Gorman, Jason.
“Dynamic characterization of in-plane bulk acoustic resonators using high-sensitivity optical reflection measurements.” Paper presented at the Hilton Head Workshop 2016:
A Solid-State Sensors, Actuators and Microsystems Workshop, Hilton Head, SC, Jun 6-Jun 9, 2016.
SP-291

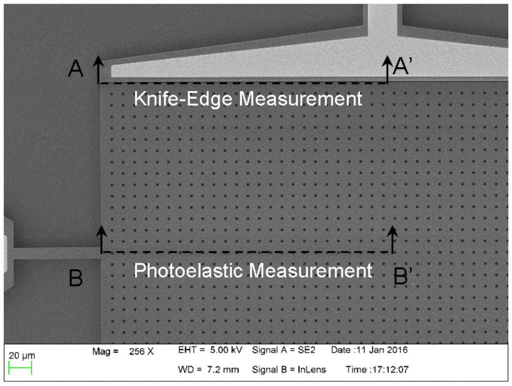


Figure 3: Optical knife-edge measurements are acquired on the free edge (AA') and photoelastic measurements are acquired on the line of maximum strain: the major axis of the device (BB').

Optical Experiment Setup

The devices are mounted on a printed circuit board (PCB) and wire-bonded. The PCB is mounted on a positioning stage with 10 nm positioning precision along all three linear axes. The SiBAR is actuated by an RF signal from the VNA and a DC bias applied to the body of the resonator. An intensity stabilized helium-neon laser is used as the optical probe ($\lambda =$ 632.8 nm). The laser is focused on the resonator surface using a 20X objective mounted on a tube microscope, resulting in a Gaussian spot on the device with a diameter of ≈ 2 µm. The reflected optical signal is detected using a Si PIN photodetector with half-power bandwidth of 200 MHz and a gain of 2000 V/W at 633 nm. The photodetector output is fed back to the VNA to provide an output signal relative to the input RF drive signal. The laser output is attenuated using a polarizer to maximize the signal from the photodetector while limiting the local heating due to the photothermal effect. Precise targeting of the laser spot is achieved by viewing the system in real time with a CCD camera on the microscope, and by monitoring the average output power reflected from the resonator using an oscilloscope. The same experimental setup is used for both optical methods and no recalibration or modification is necessary.

Knife-Edge Measurements

Optical knife-edge techniques have been used in the past to measure flexural and bulk acoustic resonators [5, 6]. This technique has the potential to measure displacements on the order of 1 pm /√Hz [6] and below. The measurements are performed by positioning a focused laser spot on any edge of the resonator surface that has high in-plane displacement. The motion of the edge modulates the reflected optical power, leading to a strong signal at the motion frequency. The leading edge of the SiBAR (AA' from Fig. 3) has minimal strain and maximum displacement along the actuation axis. The laser spot is optimally positioned at the point of maximum displacement sensitivity by scanning the spot across the gap and monitoring the photodetector output. As the leading edge of the resonator is driven to move in plane, the change in reflected power is determined by the displacement of the edge. Fig. 4 shows the magnitude and phase of the optical knife-edge signal from the resonator. The inset illustrates the knife-edge scheme and the positioning of the laser spot. Unlike electrical characterization, this method can be used to extract the absolute displacement of every point on the leading edge of the resonator by scanning the laser over the entire edge. In general, this technique can be extended to measure planar displacement on any edge with optical contrast, such as etch holes and electrodes on a piezoelectric resonator.

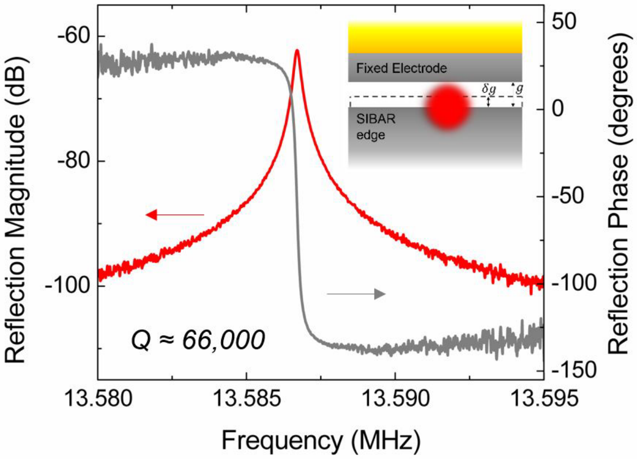


Figure 4: Reflected knife-edge signal when the laser is focused on the leading edge of the resonator (i.e., point of highest displacement and zero strain). A clear signal is acquired (both magnitude and phase), with an SNR better than 30 dB. The resonator was actuated with 10 mW RF power and 10 V DC bias in vacuum at 1.33 mPa (10 µTorr). Inset: Diagram showing knife-edge measurement with position of the laser spot (not to scale).

Measurements can be acquired on edges of any orientation, allowing displacement measurements along any planar vector. Thus the vector displacements of many points on the resonator can be measured to reconstruct the device dynamics. The measurement SNR is a function of the optical contrast between the resonator and the free space gap. For this SiBAR, the contrast is between the resonator body and the transduction trench (480 nm wide, 12 µm deep). For the current measurement, an SNR of ≈ 15 dB is achieved at DC bias levels as low as 1 V, and up to 40 dB has been measured at higher voltages. The optical contrast can be improved by removing the substrate under the trench, or by using materials with dissimilar reflectivities for the resonator and the substrate.

Photoelastic Strain Measurements

Another optical method for characterizing the dynamics of high frequency resonators is to utilize the photoelastic effect, in which the index of refraction for the resonator material is modulated by strain-inducing acoustic waves. This technique has been used in the past to measure the propagation of surface acoustic waves [7]. As the resonator undergoes periodic in-plane strain, the refractive index of the material changes at the same rate, which in turn modulates the reflected intensity of the laser spot. The change in refractive index as a function of the dynamic strain is given by $\Delta n = -\left(0.5n^3 p_{ij}\right)\Delta\varepsilon_{ij}$, where n is the nominal refractive index, p_{ij} is the set of photoelastic coefficients for the material, and $\Delta\varepsilon_{ij}$ is the change in strain [7]. Most significantly, this technique does not require an edge with optical contrast and can be used on unpatterned surfaces. A single material with uniform optical properties and a clean flat surface is the ideal platform for performing photoelastic measurements. The advantage of using a single crystal silicon device such as the SiBAR is that the photoelastic coefficients of the material are well known, thus enabling the extraction of absolute planar strain at any point on the surface. The largest surface strain in the resonator is located along the central line (BB' from Fig. 3). Representative amplitude and phase data are shown in Fig. 5. As with knife-edge measurements, the photoelastic measurements can be taken at multiple points on the surface in order to generate a composite vector plot of the surface strain dynamics of the resonator.

Gokhale, Vikrant; Gorman, Jason.
"Dynamic characterization of in-plane bulk acoustic resonators using high-sensitivity optical reflection measurements." Paper presented at the Hilton Head Workshop 2016: A Solid-State Sensors, Actuators and Microsystems Workshop, Hilton Head, SC, Jun 6-Jun 9, 2016.
SP-292

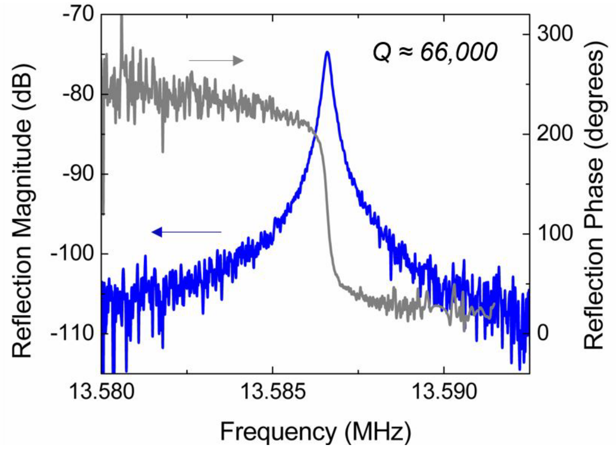


Figure 5: Photoelastic measurement at a point along the major axis of the resonator. It is clear that there is strong intensity modulation at the resonance frequency. Both magnitude and phase information are shown, with an SNR of ≈ 25 dB for the magnitude. Same test conditions as in Fig. 4.

Mode Shape Identification

A major advantage of using these two optical techniques is that they provide spatially-resolved measurements across the entire resonator, thereby enabling reconstruction of the vibration mode shapes. The fundamental mode shape along the leading edge of the SiBAR was measured with the knife-edge technique and the strain profile along the center axis of the SiBAR was measured with the photoelastic technique. These results are compared with those from FEA simulations in Fig. 6. While there is some qualitative agreement between the expected and measured mode shape and strain profile, the differences are large enough to indicate that either the measurement, the simulation, or both are inaccurate. Due to the simplicity and repeatability of the optical measurements, we believe that the FEA model is the less accurate of the two due to unmodeled fabrication imperfections and the meshing complexity of the etch holes. This assertion is supported by our observations of mode suppression and a significant loss of transduction efficiency that were not predicted by the FEA simulations.

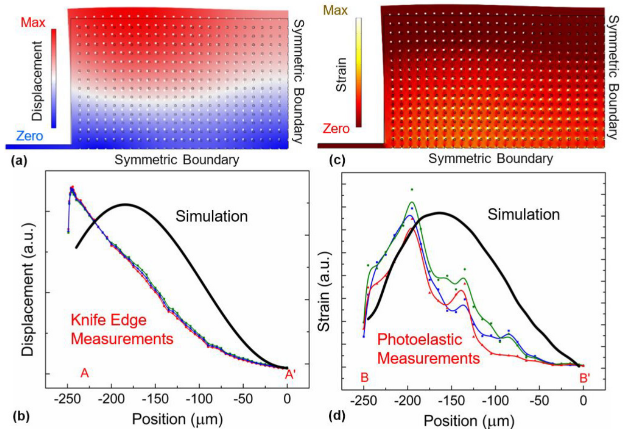


Figure 6: Fundamental mode shape and dynamic strain for the SiBAR. (a) modal displacement from FEA, (b) planar displacement along AA' (measured and simulated), (c) strain profile from FEA, and (d) photoelastic strain measurement along BB' (measured and simulated). Same test conditions as in Fig. 4. Simulation deformations and color scales are exaggerated for visual effect. Data in (b) and (d) are normalized to show the qualitative fit.

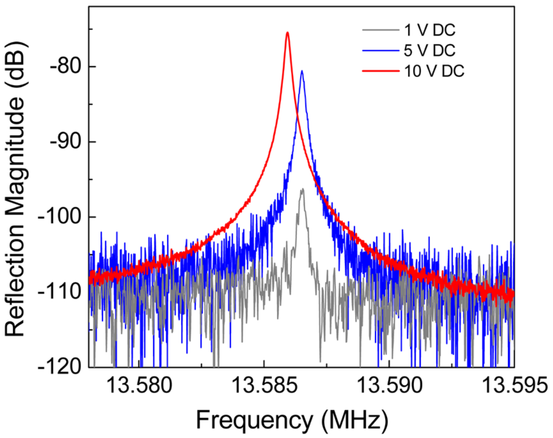


Figure 7: Knife-edge measurements as a function of DC bias. Unlike the electrical data, optical measurements have high SNR even at very low DC bias. Furthermore, optical readout is limited only by the noise in the optical path and not by device and wafer parasitics. Same test conditions as in Fig. 4.

Actuation at low drive levels

The optical techniques discussed above have far higher sensitivity to displacement and strain than the electrical measurements for the tested resonator. Within the range of 10 MHz to 100 MHz, motion can be detected at a DC bias as low as 1 V. An SNR of at least 15 dB was achieved throughout our measurements (Fig.7). The low drive voltage reduces the likelihood of inducing nonlinearities and heating, and does not require signal amplification electronics. The optical methods also make it possible to investigate thermomechanical noise in resonators and RF self-actuation. Lower RF power does not change the response magnitude, but does make the measurement noisier.

Higher Modes and Frequency Limits

The analysis above is presented for a 13.6 MHz SiBAR, which is well within the measurement limits of the presented system. The current configuration is bandwidth limited by the photodetector (200 MHz bandwidth). SiBARs with fundamental resonance frequencies up to 120 MHz have been measured with SNR ≈ 30 dB and fundamental frequencies up to 220 MHz have been detected. Higher harmonic resonance modes can also be measured with ease. Figure 8 shows the first four odd-numbered in-plane vibration modes for a SiBAR with a fundamental frequency of 28 MHz. The data shown here was measured using the knife-edge technique. We expect that the true bandwidth limits of the measurement system will be set by a combination of the decreasing displacement and strain magnitudes and increasing detector noise as the operating frequency increases. Ongoing and future experiments involve detailed system and device characterization using photodetectors operating up to 9 GHz, and will be presented elsewhere.

Signal Magnitude and Quality Factor

The magnitude of the reflected signal is a direct indicator of the displacement or strain. As such it varies over the surface of the resonator, enabling mapping of these quantities and a reconstruction of the dynamics of the resonators. For the presented SiBAR, which is fairly large, the displacement signal is stronger and less noisy than the strain signal. For smaller SiBARs, with higher frequencies and lower absolute displacements, we expect that the strain signal will be stronger than the displacement signal.

“Dynamic characterization of in-plane bulk acoustic resonators using high-sensitivity optical reflection measurements.” Paper presented at the Hilton Head Workshop 2016: A Solid-State Sensors, Actuators and Microsystems Workshop, Hilton Head, SC, Jun 6-Jun 9, 2016.

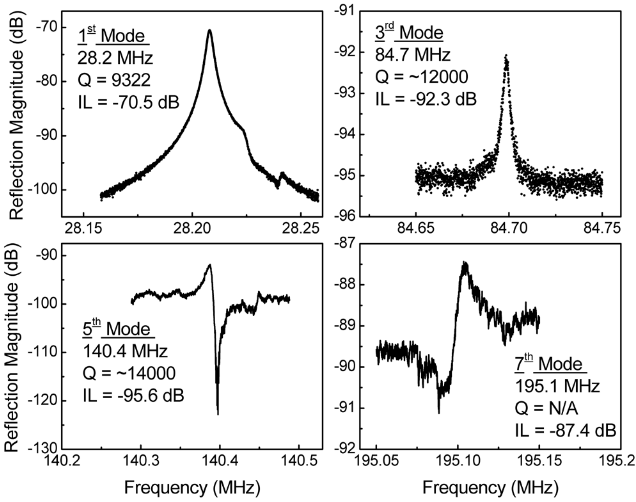


Figure 8: Fundamental width-extensional resonance and the first three odd-numbered higher modes for a SiBAR with a width of 150 µm. All modes are measured using the knife-edge technique. The resonator was actuated with 10 mW RF power and 10 V DC bias in air. The bandwidth of the photodetector prevents measurement of modes higher than 200 MHz.

Both measurements provide the same quality factor (Q) values, at any point on the resonator, within the experimental error. This Q is the direct mechanical Q of the SiBAR, and is an indicator of the intrinsic and design dependent mechanical dissipation processes (i.e., phonon loss, electron loss, thermoelastic damping, viscous damping, and tether loss). As such, these methods provide a more accurate way to measure and isolate the various dissipation mechanisms than using the 'loaded' Q values found in electrical measurement techniques. For the current SiBAR, viscous damping (due to etch holes and the transduction gaps) limits the Q to $\approx 10{,}000$ in air, and thermoelastic damping, which is exacerbated due to the etch holes, limits the Q to $\approx 66{,}000$ in vacuum [8]. It is expected that higher frequency designs, without etch holes and operated in vacuum, will allow us to mitigate these dissipation mechanisms. The Q of resonators with higher frequencies is expected to be limited by tether loss and phonon loss. The presented optical techniques will be used to study these loss mechanisms in future work.

Convolved Strain and Displacement Measurements

It is important to note that knife-edge and photoelastic measurements can be convolved when there is high strain along an edge, such as the edges of an etch hole. The strain at the leading edges of the SiBAR approaches zero so the presented knife-edge measurements were not influenced by the photoelastic effect. This was verified by measured data at points just inwards of the free edge that have near-zero photoelastic response. Conversely, at any 'solid' surface on the resonator there is no knife-edge signal, and any response is purely photoelastic. The deconvolution of the two signals based on analytical models for optical reflection will be addressed in future work.

CONCLUSION

Two complementary optical reflection measurement techniques for motion metrology of high frequency in-plane MEMS resonators were presented. The knife-edge technique can be used to measure planar displacement on any device edge with optical contrast, while the photoelastic measurement technique can be used on any clean solid material that has reasonable photoelastic coupling. Both techniques provide high sensitivity and resolution as compared to contemporary electrical methods, and are simpler to set up and use than other solutions such as 3D laser vibrometry. These techniques can be used to reconstruct the vibration mode shapes of resonators, allowing MEMS designers to better understand and optimize their designs for improved performance. These techniques also provide a more sensitive way to measure the mechanical dissipation in high frequency resonators, and can provide a path to a better experimental understanding of dissipation, even making it possible to separate and isolate different underlying dissipation mechanisms. The initial set of experiments with SiBARs indicates that there are differences between the measured and simulated mode shapes that cannot be easily explained. The possible causes for these differences and their effect on the performance of the resonator are topics of ongoing and future investigation.

REFERENCES

[1] S. Pourkamali, A. Hashimura, R. Abdolvand, G. K. Ho, A. Erbil, and F. Ayazi, "High-Q single crystal silicon HARPSS capacitive beam resonators with self-aligned sub-100-nm transduction gaps," *Journal of Microelectromechanical Systems,* vol. 12, pp. 487-496, Aug 2003.

[2] G. Piazza, P. J. Stephanou, and A. P. Pisano, "Piezoelectric aluminum nitride vibrating contour-mode MEMS resonators," *IEEE Journal of Microelectromechanical Systems,* vol. 15, pp. 1406-1418, Dec 2006.

[3] B. Gibson, K. Qalandar, K. Turner, C. Cassella, and G. Piazza, "Analysis of the impact of release area on the quality factor of contour-mode resonators by laser Doppler vibrometry," in *Frequency Control Symposium & the European Frequency and Time Forum (FCS), 2015 Joint Conference of the IEEE International*, 2015, pp. 709-712.

[4] C. Rembe, R. Kowarsch, W. Ochs, A. Dräbenstedt, M. Giesen, and M. Winter, "Optical three-dimensional vibrometer microscope with picometer-resolution in x, y, and z," *Optical Engineering,* vol. 53, pp. 034108-034108, 2014.

[5] L. Jaesung, L. Cheng-Syun, L. Ming-Huang, C. Chi-Hang, L. Sheng-Shian, and P. X. L. Feng, "Multimode characteristics of high-frequency CMOS-MEMS resonators," in *Frequency Control Symposium (FCS), 2014 IEEE International*, 2014, pp. 1-3.

[6] D. Karabacak, T. Kouh, C. C. Huang, and K. L. Ekinci, "Optical knife-edge technique for nanomechanical displacement detection," *Applied Physics Letters,* vol. 88, p. 193122, 2006.

[7] L. Shao, M. Zhang, A. Banerjee, P. K. Bhattacharya, and K. P. Pipe, "Electrically driven nanoscale acoustic source based on a two-dimensional electron gas," *Applied Physics Letters,* vol. 103, p. 083102, 2013.

[8] C. Tu and J. E.-Y. Lee, "Increased dissipation from distributed etch holes in a lateral breathing mode silicon micromechanical resonator," *Applied Physics Letters,* vol. 101, p. 023504, 2012.

ACKNOWLEDGMENTS

Research was performed in part in the NIST Center for Nanoscale Science and Technology Nanofab.

CONTACT

*Jason J. Gorman, tel: +1-301-975-3446; gorman@nist.gov

Gokhale, Vikrant; Gorman, Jason.
"Dynamic characterization of in-plane bulk acoustic resonators using high-sensitivity optical
reflection measurements." Paper presented at the Hilton Head Workshop 2016:
A Solid-State Sensors, Actuators and Microsystems Workshop, Hilton Head, SC, Jun 6-Jun 9, 2016.

Measuring and Characterizing Tris (2-chloro-1-methylethyl) Phosphate Emission from Open Cell Spray Polyurethane Foam

Dustin Poppendieck
Mengyan Gong

Engineering Laboratory, National Institute of Standards and Technology
100 Bureau Drive Gaithersburg, MD 20899

Content submitted to and published by:
14th International Conference on Indoor Air
Quality and Climate Conference

U.S. Department of Commerce
Penny Pritzker, Secretary of Commerce

National Institute of Standards and Technology
Willie E May, Director

NIST National Institute of Standards and Technology • U.S. Department of Commerce

SP-295

DISCLAIMERS

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Any link(s) to website(s) in this document have been provided because they may have information of interest to our readers. NIST does not necessarily endorse the views expressed or the facts presented on these sites. Further, NIST does not endorse any commercial products that may be advertised or available on these sites.

Measuring and Characterizing Tris(2-chloro-1-methylethyl) Phosphate Emission from Open Cell Spray Polyurethane Foam

Mengyan Gong[1], Dustin Poppendieck[1*]

[1]Indoor Air Quality and Ventilation Group, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899-8633, USA

[*]*Corresponding email: dustin.poppendieck@nist.gov*

SUMMARY

Understanding emission of Tris(2-chloro-1-methylethyl) Phosphate (TCPP) from spray polyurethane foam (SPF) insulation will contribute to the assessment of exposure to TCPP in indoor environments. This study aims to: (1) develop a method to determine the gas phase concentration of TCPP in equilibrium with the material phase (y_0) for open cell SPF, (2) determine the partition coefficient for TCPP between air and SPF (K), and (3) examine the influence of temperature on y_0 and K. The emission of TCPP from two kinds of open cell SPF in a closed micro-chamber without flow are being tested. The steady-state gas phase TCPP concentration in the chamber (C_{equ}) is also being measured. C_{m0} (the initial concentration of TCPP in SPF) is measured using a solvent extraction method. C_{equ} and C_{m0} will then be used to determine y_0. These measurements are still in progress, and the preliminary results will be presented at the conference.

PRACTICAL IMPLICATIONS

The parameters (y_0 and K) derived in present study can be used to predict TCPP emission from SPF in full scale indoor environments.

KEYWORDS

TCPP, Flame Retardant, Indoor Environment, Exposure, Spray Polyurethane Foam

1 INTRODUCTION

The desire to create more energy-efficient buildings in the United States has increased the application of spray polyurethane foam (SPF) insulation to reduce building envelope heat loss. Two different kinds of SPF, open cell (low density) and closed cell (medium density), can be produced on site via an exothermic reaction of two sets of chemicals. One of the main components in SPF is the flame retardant Tris(2-chloro-1-methylethyl) Phosphate (TCPP), which can be present in foam at a concentration up to 12 % by mass (Sebroski, 2012). Since TCPP is not chemically bound to the polymer matrix, TCPP may be emitted from the SPF after installation. Exposure to TCPP has been associated with asthma, reproductive and developmental problems (USEPA, 2014). Understanding the emission of TCPP from SPF will contribute to the assessment of exposure of TCPP in indoor environments and the development of strategies to control potential exposures. Previous studies have shown that emission of TCPP is likely externally controlled (convection) for open cell SPF, while it is controlled by both internal diffusion and convective process for closed cell SPF (Poppendieck et al., 2016). This study aims to measure the emission parameters of TCPP (y_0 and K) from open cell SPF and examine the influence of temperature on those parameters.

2 MATERIALS/METHODS

Figure 1 shows the schematic of chemical emission from SPF in a closed chamber. Based on mass balance at equilibrium:

$$V_m C_{m0} = K V_m C_{equ} + V_a C_{equ} + K_s A_s C_{equ} \quad (1)$$

Where, C_{m0} is the initial concentration of TCPP in SPF (μg/m^3), V_{m} is the volume of SPF (m^3), K is the partition coefficient for TCPP between air and SPF, C_{equ} is the equilibrium TCPP concentration in air (μg/m^3), V_{a} is the volume of air in the chamber (m^3), K_{s} is the partition coefficient of TCPP between the chamber wall and air, and A_{s} is the area of adsorption surface (m^2).

- C_{equ} is measured using a 1 L chamber and thermal desorption-gas chromatograph/mass spectrometer (TD-GC/MS) system. A small piece of SPF is placed in the chamber (Figure 2). The air concentration in the chamber can be measured by taking a 10 mL sample. When the concentration difference between two successive samples (sampled every hour) is less than 5 %, the emission process is considered to have reached equilibrium and the measured concentration is used as C_{equ}.

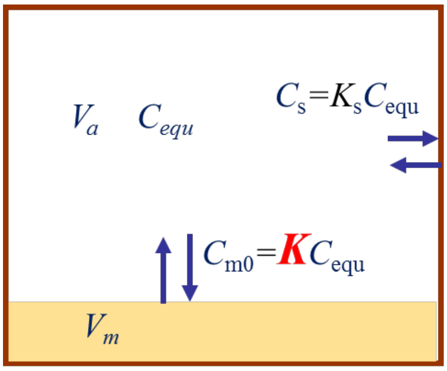


Figure 1 Emission process in a closed chamber

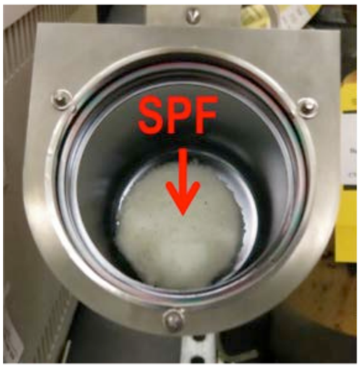


Figure 2 Photo of the chamber

- C_{m0} is measured by cutting the SPF into small pieces, extracting the sample ultrasonically with hexane/methanol four times and measuring the TCPP concentration in the extract using GC-MS.
- V_{m} is calculated based on the mass and the measured density of the SPF. V_{a} is calculated by substracting V_{m} from the total volume of the chamber (1L).
- Since C_{m0} is very large in SPF (around 10^9 μg/m^3), $KsAsC_{\mathrm{equ}}$ is negligible compared to $V_{\mathrm{m}}C_{\mathrm{m0}}$ and can be removed from equation (1). Then K can be calculated, if C_{equ}, C_{m0}, V_{m}, and V_{a} are known. The gas phase concentration in equilibrium, y_0 can be calculated as C_{m0}/K.

3 RESULTS AND DISCUSSION

These measurements are still in progress. Preliminary results will be presented at the conference.

4 CONCLUSIONS

The parameters (y_0 and K) derived in the present study can be used to predict TCPP emission from SPF in indoor environments.

5 REFERENCES

Poppendieck, D.; M. Schlegel; A. Connor; A. Blickley. Flame retardant emissions from spray polyurethane foam insulation” ASTM Selected Technical Papers, 2016, accepted for publication.

Sebroski, J. R. Research report for measuring emissions from spray polyurethane foam (SPF) Insulation; Center for the Polyurethanes Industry (CPI): Pittsburgh, PA, September 4, 2012.

USEPA. Flame retardants used in flexible polyurethane foam: an alternatives assessment update. In Environment, D. f. t., Ed. U.S. EPA: 2014.

On the Internet Connectivity in Africa

Assane Gueye[a], Peter Mell[b], Desire Banse[b], and Faical Y. Congo[b]

[a]University of Maryland, College Park (agueye@umd.edu)

[b]National Institute of Standards and Technology, Gaithersburg
(peter.mell|desire.banse|faical.congo@nist.gov)

Abstract[1]. This study measures growth of Internet connectivity in Africa from 2010 to 2014 with a focus on inter-country relationships. An initial analysis reveals a modest increase in the number of participating countries but an explosive increase in the number of routers and network links. We then form the first country level topology maps of the African Internet and evaluate the robustness of the network. We study raw connectivity, pairwise shortest paths, and betweeness centrality, suggesting how improvements can be made to the inter-country African connectivity to enhance its robustness without reliance on paths traversing multiple continents.

Keywords: Africa, Internet, Connectivity, Measurement

1. INTRODUCTION

As recently as 2007, more than 70 % of internal African Internet traffic was routed to other continents (generally Europe) before reaching its final African destination [1]. This statistic suggests that internal African Internet connectivity was composed of non-communicating isolated clusters. This was true despite the existence of fiber optic submarine cables circling the entire continent [2]. In this study we measure and document the growth of the African Internet with respect to connectivity from 2010 to 2014. We show how the African Internet is losing its fractured nature and is strengthening in its robustness to connectivity disruptions. We first focus our measurements on router to router connectivity and observe a consistent imbalance in the density of Internet infrastructures between different countries. Supporting this is a 2013 observation that 80% of the hosts in Africa were in the country of South Africa [3]. To avoid biasing our analysis toward countries with this high density, we create a novel country-to-country connectivity map of Africa. With this approach, we evaluate the connectivity of individual countries to each other and thereby measure more uniform growth.

We form our African country connectivity graphs by leveraging publicly available data from the Cooperative Association for Internet Data Analysis (CAIDA) [4]. CAIDA provides us router level topological maps of the Internet with embedded geolocation information. CAIDA continuously updates its IP level topological map through the employment of its Archipelago (Ark) measurement infrastructure. As of 2014-05-09, Ark had 94 monitors distributed worldwide, separated into three teams. Every 2 to 3 days, each team uses a traceroute-like procedure to probe a random IP address within each /24 subnet in the IPv4 address space. This yields a list of routers connecting the monitor to the target IP. With this architecture, the Ark infrastructure is only capable of discovering preferred paths to and from subnets containing a monitor. Routes between subnets that do not lie on a preferred route from a monitor to a target subnet will not be discovered. However, over time, each subnet is accessed from many different parts of the world (both countries and continents), revealing the primary pathways through the Internet. Thus, we have confidence that we are discovering the major pathways through Africa. Because of this limitation, however, our resulting connectivity analyses should be considered as worst case bounds given that some smaller pathways between countries may not have been

[1] This work is a part of NIST efforts to develop metrics and tools for the analysis of complex interconnected systems with emphasis on the study of the resilience of critical infrastructure.

detected. Using the geo-location data files provided by CAIDA, we label each router with its country. Each file provides an incomplete map of routers to locations (including country codes) over a certain time period. For each router, the file creators examine the location information for all its interfaces. If all of them map to the same location, then they label the router with the respective location (and most importantly to us, the respective country). For each router for which a country label is not available, we label it with the country label that is most common among its neighbors. If there is a tie between two or more countries, we make a random assignment. In rare cases where none of a router's neighbors have country labels, we perform a breadth first search and find the closest labelled router and use its country label. With this procedure, almost all nodes (except a tiny fraction ~0.0001%) were assigned a geo-location. We lastly form a country level topology map from the router level topology map by merging nodes with identical country labels. Lastly, we represent the non-African continents as single nodes by merging all non-African country nodes into nodes representing their respective continents. The end result is communication interconnectivity graphs for Africa from 2010 to 2014 showing each country as a separate node and each non-African continent as a node (all multi-edges are removed). We then study country connectivity within Africa by evaluating raw connectivity, pairwise shortest paths, and betweenness centrality.

2. DATA ANALYSIS

Figure 1 shows the number of routers observed within Africa during the measurement period. The 'A-Nodes' line represents the number of routing nodes in Africa. The 'AA-Links' line represents the number of intra-Africa links over time. And the 'AW-Links' line represents the number of links between African routers and the rest of the world. The plots show a steady growth in the number of routers and links, indicating the growth in the overall infrastructure of the African Internet. This growth begins after October 2011 and continues through 2014 representing a factor of 35 increase in the number of routers observed in Africa. The number of observed links to other continents has also increased, but less significantly. The number of observed countries rises from 54 in 2010 to 57 in 2013 (all countries in the mainland). For the inter-country African links, we see a factor of 5 growth from 2010 to 2014, showing significant growth. However in 2014, these links accounted for only 0.3% of the links where both routers reside within Africa. Thus, the number of these critical inter-country links is relatively small but growing rapidly. In 2014, the African routers represent about 1.6% of the world's routers (and 1.2% of the world's links). Africa's share of worldwide routers and links modestly increases over the period of investigation while the fraction of world links that connect Africa to the other continents has stayed steady since 2010 (not shown). Taken as a whole, the data indicates that most of the effort to improve Africa's connectivity has been spent to connect nodes inside Africa. However, the countries with the greatest share of routing infrastructure have seen the most growth while the countries with the smallest share have experienced much smaller growth. Table 1 shows this disparity. The 'top 3 countries' (South Africa, Egypt, and Morocco) are those with the greatest number of nodes/links in 2014 while the 'bottom 24 countries' are those with the fewest nodes/links in 2014. Similar observations were made in reference [3] for the period 2004-2007 showing that this is a long term trend (although in this earlier period South Africa drove the majority of the growth).

Table 1: Improvement in the number of links and nodes in Africa from 2010 to 2014.

	Continent	Top 3	Bottom 24	Rest of Africa
Nodes	**35x**	**46x**	**6x**	**17x**
Links	**12x**	**15x**	**6x**	**7x**

To avoid biases involving countries with more infrastructures we now evaluate the country level interconnectivity maps. Figure 2 shows the number of country-level links within Africa and between Africa and the rest of the world. Figures 3-6 show a graphic representation of the country-level connectivity for part of the investigation period. As was already seen at the router level, the number of country level links within Africa is increasing but it is always smaller than the number of country-level links to the rest of the world. This indicates that even though Africa is improving its connectivity at the country level, it largely depends on the other continents (or satellite) for Internet connectivity. In 2010 and 2011, a number of African countries (24%) were connected via satellite (VSAT or directly to a country in a different continent) and do not have any direct link to other African countries. This was mostly the case for inland countries. Coastal countries (especially in the western part of the continent) are almost all directly connected to the Internet. One reason could be the deployment of the SAT3/WASC (South Atlantic 3/West Africa Submarine Cable) fiber optic submarine cable which goes along the west coast, giving countries in that coast an easier access. East coast countries are also connected to the Internet (possibly through the East Africa Submarine Cable System—EASSy). Another reason of this lack of infrastructure in landlocked countries is related to investment. According to African Economic Outlook, [7] resource scarce landlocked countries in Sub-Saharan Africa have attracted the lowest volume of investment in telecommunication during the period 2000-2007. In 2014, the African country-level graph is connected (except for some island countries), implying that any African country can now communicate with any other African country using only links within the continent.

We now study the characteristics of the country level connectivity graph. Figure 7 shows histograms of the country to country degree distribution for year 2014 (all other measurement periods present similar characteristics). Most countries (always more than 25) have low degree, while a few countries (mostly South Africa) have high degree (greater than 20). The many low degree nodes and few high degree nodes is a characteristic of many engineered networks [5] and is usually referred as '*scale-free*'. Furthermore, we observed that nodes with low degrees tend to connect with nodes with high degree, and vice versa. This is another previously observed property of engineered networks and is referred as '*dissassortativity*'[6]. Another metric of interest is the '*betweenness*' centrality of individual countries, the fraction of shortest paths that go through that country (among pairs of African countries). Figure 8 shows that the majority of countries have very low betweenness centrality (carrying very little "relay" traffic). Only a small number of countries have a significant betweenness centrality. This indicates that if inter-country traffic is routed using shortest path, only a few African countries will play a role of big hubs, while most countries will carry only traffic which they have generated or which is destined to them. Also, the average number of hops between any pair of countries is always greater than 1 during the measurement period (in contrast, it is 0.5 for Europe). This means that, in average, communication between any pair of African countries has to transit through a third African country (while, in average, countries in Europe have direct link to each other).

We next study the robustness of the country-level Africa graph to node and link failures. There exist several graph theoretic metrics to quantify the importance of a node (or link) in a network: (a) the degree of a node, (b) the betweenness of a node which quantifies how often a node lies in the shortest path between other nodes that represent the source and destination of a communication, and (c) the eigenvector centrality of the node which measures how connected the node is to well-connected nodes (the higher it is, the more connected the node is to well-connected nodes). Since all these features are important in the connectivity of a given country, we combine them with the formula $Conn(c)=(\mathrm{Deg}(c)+Bet(c))e^{\mathrm{Eig(c)}}$ to define the connectivity of a country where Deg(c) is the degree of the country, Bet(c) is the betweenness of the country and Eig(c) is its eigenvalue centrality. We define the connectivity of the continent as the sum of the connectivity of its countries. We then use this metric to study the robustness of the Africa network to node and link failures by asking the following question: what is the maximum drop in connectivity when 1 (2,3,4,..) node (resp. link) of the network fails? Figure 9 shows the evolution of the continent connectivity when we allow up to 5 countries to fail. For each of the number of nodes (allowed) to fail, we sequentially remove the node with largest drop in connectivity. We observe a very sharp decline for the first two countries and then the connectivity decreases at a slower rate. This suggests that the first two countries are very important for the connectivity of the continent as a whole. Similar analysis for link failures shows an almost linear drop in connectivity as more links fail (not shown).

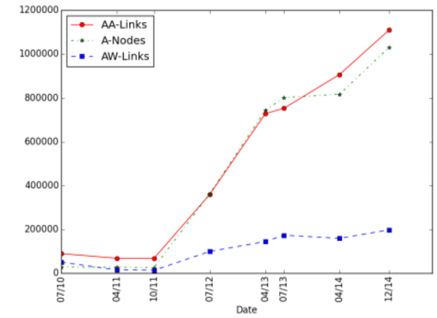


Figure 1: Number of nodes in Africa and number links within Africa and between Africa and the rest of the world.

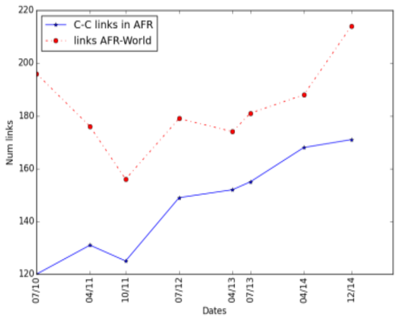


Figure 2: Number of country-level links within Africa and between Africa and the rest of the world.

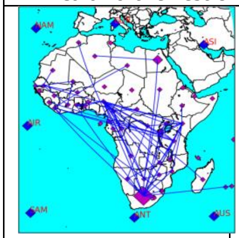


Figure 3: 2010-07

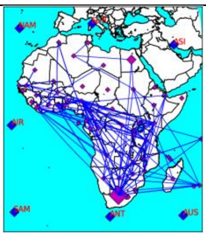


Figure 4: 2011-07

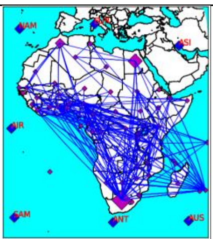


Figure 5: 2013-07

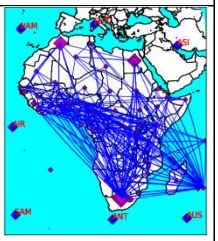


Figure 6: 2014-12

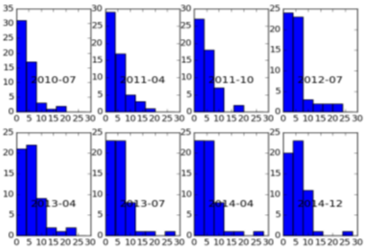


Figure 7: Number of connections for countries within Africa.

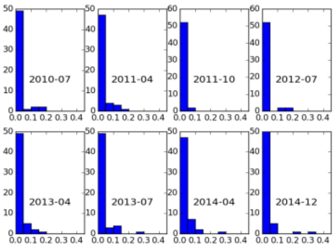


Figure 8: Betweenness centrality.

Finally, we propose an improvement of Africa's connectivity by adding new links to the country-level graph. For each additional link, we ask the question: where in the continent (i.e., between which pairs of countries) to put the link to obtain the maximum increase in connectivity. We assume that there are 19 links to be added sequentially. For each new link, we use the connectivity metric defined above to compute its best placement (i.e., which has a maximum increase in connectivity). Figure 10 shows the improvement in the continent connectivity after the addition of each optimally placed link. We can see that the connectivity improves as more links are being added. However, the curve has a few plateaus (between 5 and 8 additional links, between 10 and 12, and after 15) between which its increases. One interpretation is that after having added 5 (resp. 10) links in the continent, one does not gain much by adding more links except if one can add at least 3 (2) additional nodes. This pattern of flat region-increasing region repeats even beyond 20 links (not shown). We also see that connecting nodes that already have many connections results in a smaller payoff while connecting nodes with small number of connections results in large payoff. In other words, in order to improve Africa's connectivity, we need to build links between countries with less Internet infrastructure.

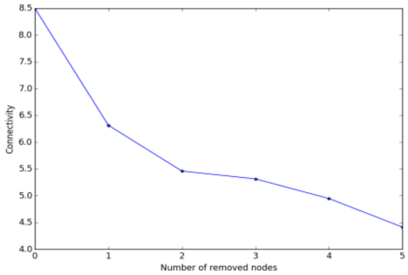


Figure 9: Robustness to node failures.

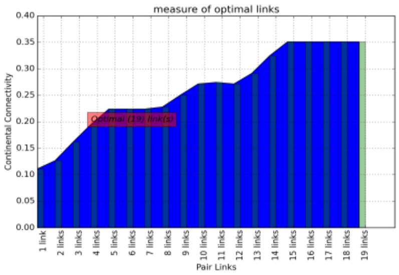


Figure 10: Improving by adding links.

3. RELATED WORK

Several studies are available showing African Internet accessibility (see [2] and [7]). The African Economic Outlook [7] provides and analyzes data on telecommunication investments, access to information technology, technology penetration, and connectivity in Africa. They have reported 16 undersea cables connecting Africa to the Americas, Europe and Asia (e.g., SAT3/WASC, EASSy, Seacom, TEAMS, RCIP, GL01, MaIN, ACE). With the exception of Eritrea and Western Sahara, all coastline countries have a cable landing on their shore. This has helped triple the Africa Internet access in the last decade. On the other hand, landlocked countries were (up to 2010) mainly connected via satellite (VSAT). However, our data shows that this is changing with inland countries connecting to the undersea cable via fiber optic cables traversing neighboring coastline countries. Most of the observations in [7] are also made in this paper, although it is based on (different) topological data set. Our paper, however, goes one step further by introducing a novel country-level connectivity graph of Africa and studies its properties. We also investigate improvement to the current country-level connectivity. [8] provides an analysis of the distribution of Internet infrastructure in Africa for the years prior to our study (with some of the same trends being found with respect to a few countries dominating African network growth). The ping end-to-end reporting (PingER) project is, like CAIDA, an Internet End-to-end Performance Measurement (IEPM) project that monitors end-to-end performance of Internet links [9]. Using the simple and common "ping" test, PingER regularly measures how well data is flowing, if at all, between pairs of hosts. [10] uses PingER to shown the low presence of Africa in the world Internet, a steady improvement of Africa connectivity since late 2010, and the disparity in improvement among the African countries. Our study, although based on a different data set, confirms such observation. Their paper, however, does not study country-level connectivity nor does it consider the robustness and improvement analyses carried in our study.

4. CONCLUSION

The development of the African Internet has lagged behind more developed continents. However, in the period of study from 2010 to 2014, significant growth has been observed. While our data source for this study certainly contains missing data (not all routes are visible), we have been able to evaluate rising lower bounds that indicate significant improvements throughout Africa. The raw data indicates that the fraction of worldwide Internet backbone routers attributable to Africa is increasing. Furthermore, the number of intra-Africa links has risen substantially which is important given that much of the African inter-country connectivity had been previously routed through other continents. On a downside, we note that most of the router growth occurred in African countries that already had a robust infrastructure. That said, the countries with less infrastructures also generally experienced Internet infrastructure growth during the time period of study. Moving beyond analyzing the raw data, we developed a novel country to country connectivity map of Africa. This enabled us to overcome analysis biases that can arise due to the bulk of Internet infrastructure residing in just 3 countries. With this map, we see an increasing participation of African countries over the time period of study. We also see a significant increase in the number of direct links between African countries. Even with these added links, however, the connectivity is still not as robust as Europe where the average hop length is much less. With respect to the rest of the world, we see an increase in links from African countries to other continents. At a deeper level, our connectivity metrics also reveal a highly scale free nature in the country to country Africa connectivity graph. There are many countries of low degree and a few of high degree. There is a negative assortativity whereby the low degree nodes tend to connect to the high degree nodes and not to each other. The connectivity within the center of Africa tends to be low. The problem with this this current architecture is that it is susceptible to node failure. The majority of African countries are dependent upon just a few other African countries for their intra-continental Internet access. However, judicious placement of additional links can reduce the fragility induced by the scale free nature (i.e., links among the low degree nodes). This translates in the need for direct Internet links between countries with less Internet infrastructure in order to make that African Internet stronger as a whole.

5. ACKNOWLEDGEMENTS

This research was sponsored by the National Institute of Standards and Technology (NIST) and partially accomplished under NIST Cooperative Agreement No.70NANB13H012 with the University of Maryland. The views and conclusions contained in this document should not be interpreted as representing the official policies, either expressed or implied of NIST or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes, notwithstanding any copyright notation hereon.

6. REFERENCES

[1] "Africa Waiting for Net Revolution", BBC News, [Onilne]. Available: http://news.bbc.co.uk/2/hi/technology/7063682.stm [Accessed 7/13/15]

[2] International Telecommunication Union: Telecommunication/ICT Markets and Trends in Africa, 2007. [Online]. Available: http://www.itu.int/ITU-D/ict/statistics/material/af_report07.pdf [Accessed 7/13/15]

[3] Giancarlo Livraghi. Data on Internet Activity in Africa (Hostcount). [Online]. Available: http://www.gandalf.it/data/africeng.htm [Accessed 7/13/15]

[4] CAIDA. Macroscopic Internet Topology Data Kit. [Online]. Available: http://www.caida.org/data/internet-topology-data-kit/ [Accessed 7/13/15]

[5] A.-L. Barabási and R. Albert (1999) Emergence of scaling in random networks. Science 286, 509-512

[6] M. E. J. Newman, "Mixing Patterns in Networks," *Phy. Rev.*, vol. 67, no. 2, 2003.

[7] African Economic Outlook: Technology Infrastructure and Services in Africa. [Online]. Available: http://www.africaneconomicoutlook.org/en/theme/ict-africa/technology-infrastructure-and-services-in-africa/

[8] Data on Internet Activity in Africa (Hostcount). [Online]. Available: http://www.gandalf.it/data/africeng.htm [Accessed 7/13/15]

[9] Ping End-to-End Reporting (PingER). Project website: http://www-iepm.slac.stanford.edu/pinger/.

[10] R. Les Cottrell: How bad is Africa's Internet? IEEE Spectrum. [Online] Available: http://spectrum.ieee.org/telecom/internet/how-bad-is-africas-internet.

Linear Temporal Logic (LTL) Based Monitoring of Smart Manufacturing Systems

Gerald Heddy[1], Umer Huzaifa[2], Peter Beling[3], Yacov Haimes[4], Jeremy Marvel[5], Brian Weiss[6], and Amy LaViers[7]

[1,2,3,4,7] *University of Virginia, Charlottesville, VA, 22904, USA*
grh4aw@virginia.edu
muh5zc@virginia.edu
beling@virginia.edu
haimes@virginia.edu
alaviers@virginia.edu

[5,6] *National Institute of Standards and Technology, Gaithersburg, MD, 20899, USA*
jeremy.marvel@nist.gov
brian.weiss@nist.gov

Abstract

The vision of Smart Manufacturing Systems (SMS) includes collaborative robots that can adapt to a range of scenarios. This vision requires a classification of multiple system behaviors, or sequences of movement, that can achieve the same high-level tasks. Likewise, this vision presents unique challenges regarding the management of environmental variables in concert with discrete, logic-based programming. Overcoming these challenges requires targeted performance and health monitoring of both the logical controller and the physical components of the robotic system. Prognostics and health management (PHM) defines a field of techniques and methods that enable condition-monitoring, diagnostics, and prognostics of physical elements, functional processes, overall systems, etc. PHM is warranted in this effort given that the controller is vulnerable to program changes, which propagate in unexpected ways, logical runtime exceptions, sensor failure, and even bit rot. The physical component's health is affected by the wear and tear experienced by machines constantly in motion. The controller's source of faults is inherently discrete, while the latter occurs in a manner that builds up continuously over time. Such a disconnect poses unique challenges for PHM. This paper presents a robotic monitoring system that captures and resolves this disconnect. This effort leverages supervisory robotic control and model checking with linear temporal logic (LTL), presenting them as a novel monitoring system for PHM. This methodology has been demonstrated in a MATLAB-based simulator for an industry inspired use-case in the context of PHM. Future work will use the methodology to develop adaptive, intelligent control strategies to evenly distribute wear on the joints of the robotic arms, maximizing the life of the system.

1. Introduction

Industries active in the manufacturing sector exist in a competitive landscape where profitability is heavily influenced by their operational directives. A manufacturer choosing to implement Smart Manufacturing Systems (SMS) would likely drive down their costs, improve their manufacturing goals, and meet continuous improvement objectives. Robotics and automation are often a logical and feasible ingredient to increasing productivity, while also maintaining or improving product quality and operational safety goals. A recent national report on advanced manufacturing showed that industry use of automation positively impacted profitability such that manufacturers were more likely to keep their internal operations vertically integrated (Anderson, 2011). This report also highlights the important role that next-generation robotics will play in the future of manufacturing such as realizing improvements in flexibility, time to market, cost, quality, and human safety.

Prognostics and Health Management (PHM) is a comprehensive field that attempts to create the systems and methods which manufacturers employ to enhance their asset maintenance programs. PHM standards are developed as a better alternative to traditional reactive maintenance programs primarily defined by initiating action only after a breakdown or some lost production time event has occurred. It is through the use of condition-monitoring, diagnostic, and prognostic

Gerald Heddy et al. This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 United States License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Heddy, Gerald; Huzaifa, Umer; Beling, Peter; Haimes, Yacov; Marvel, Jeremy; Weiss, Brian; LaViers, Amy.
"Linear Temporal Logic (LTL) Based itoring of Smart Manufacturing Systems."
Paper presented at the Annual Conference Of The Prognostics And Health Management Society, San Diego, CA, Oct 19-Oct 24, 2015.

methods that PHM attempts to understand the states of the system and create a manufacturing environment where maintenance is carried out on a more preventative, predictive, and proactive basis as compared to being purely reactive. A PHM approach to maintenance proves beneficial by reducing manufacturer dependence on non-value added maintenance time and capital of parts replacement. PHM strives to increase asset lifespan while operating at lower cost.

The emergent contributions of robots to higher efficiency and product quality in smart manufacturing processes have also introduced new sources of risk thereto including: (i) safety risks resulting from the collaborative and proximal interface between humans and robots; (ii) maintenance schedule and operations; and (iii) sensitivity to irregularities associated with out-sourced parts and raw materials, among others. In this sense, the centrality of PHM in smart manufacturing has necessitated expansion to embrace systems-based risk modeling, assessment, management, and communication (Haimes, 2012, 2005). In particular, the interdependencies between the robotics subsystems and the human operators necessitate an understanding of the epistemological human behavior and responses under extreme events originating from either the robotics or human subsystems.

It is then necessary to think about PHM in the context of robotics as both of these fields (PHM and robotics) enable development of SMS. As private and public investment rises to implement and develop next-generation robotics, we will also need to create the high-level control strategies which seek to attain condition-based PHM goals. This work introduces a novel robotic monitoring system as a step towards PHM with the motivation to display and predict both discrete system failures and continuous motion wear.

After further review of SMS, the paper introduces an industry-inspired use case. We will then apply a novel methodology from (Huzaifa, Umer and Marvel, Jeremy A. and LaViers, Amy E., 2015) that can incorporate a high-level description of the correct behavior for the robotic system to our use-case. This is accomplished with linear temporal logic (LTL) specifications and a labeled, discrete representation of the SMS. By generating a Büchi automaton representation of the high-level specification phrased in LTL, the system dynamic and correct behavior can be represented in the same product automaton. This resulting automaton encodes all system behavior that is within the specification and forms the basis of the monitoring system. This methodology has been implemented in a MATLAB-based simulator, which also tracks a continuous system variable.

Finally, the paper presents results of this methodology with respect to PHM. Correct control sequencing is represented at a high-level using task-level labels for the discrete system model. It is over these task-level labels that the specification will monitor the correct behavior of the system. Wear monitoring is achieved using a differential equation model of wear in both loaded and unloaded conditions. These discrete and continuous statuses are tracked and displayed and will be used to develop corrective control strategies to maximize the lifetime of the robotic system. This work is part of a larger effort to create a modular, adaptive multi-scale PHM scheme (AM-PHM) where we take operational demand profiles, generate performance and health assessments, then create operational objectives.

2. PROGNOSTICS AND HEALTH MANAGEMENT FOR SMART MANUFACTURING SYSTEMS

Prognostics and health management (PHM) technologies reduce time and costs for maintenance of products or processes through efficient and cost-effective diagnostic and prognostic activities. In 2010, a comprehensive review was conducted of prognostic and diagnostic methodologies for condition-based maintenance (CBM) that presented the existing strategies within four categories: physical models, knowledge-based models, data-driven models, and combination (hybrid) models (Peng, Dong, & Zuo, 2010). This review highlighted many specific methods across these four categories (e.g., Hidden Markov Models, Bayesian network-related methods, Fuzzy Logic, Principal Components Analysis) along with their successes and limitations. No one method stood out as being sufficient to provide both diagnostic and prognostic intelligence at multiple levels. This review demonstrated that for every method's strength, there was at least a single weakness. Similarly, another review of existing methods was conducted in 2012 that focused on comparing time-based maintenance (TBM) and condition-based maintenance (CBM) (Ahmad & Kamaruddin, 2012). TBM, commonly referred to as preventative maintenance, is typically simpler to implement (in that maintenance is scheduled based upon a specific unit of time; e.g., cycle time) while CBM, sometimes termed predictive maintenance, may ultimately be more cost effective if a process's or equipment's health data accurately reflects its current state and allows a machine to run longer until maintenance (as compared to a TBM schedule). The challenge in CBM is gathering sufficient data to make a reasonably accurate prediction. Both of these studies revealed that PHM is applicable to both products and processes; this makes PHM a tremendous, and necessary, asset to SMS.

Product PHM (providing health monitoring, diagnostics, and/or prognostics for a finished system; e.g., automobile, aircraft, power generation station) is more widespread as compared to process PHM (providing health monitoring, diagnostics, and/or prognostics to a system that integrates one or more pieces of equipment to complete a task; e.g., assembly process, welding process, machining process). (Batzel & Swanson, 2009) (Holland, Barajas, Salman, & Zhang, 2010) (Hu & Koren, 1997) (Shen, Wan, Cui, & Song, 2010). Likewise, PHM techniques have been developed and applied more widely at the component/equipment level, yet some work has occurred at the higher/system levels. For example, innovative methods have been developed for various machining operations (Al-Habaibeh & Gindy, 2000) (Altintas, Verl, Brecher, Uriarte, & Pritschow, 2011) (Biehl, Staufenbiel, Recknagel, Denkena, & Bertram, n.d.) (Borisov, Fletcher, Longstaff, & Myers, 2013). System level PHM methods have also been developed, yet seem to be very focused in their applicability and/or limited in capability (Barajas & Srinivasa, 2008) (Datta, Jize, Maclise, & Goggin, 2004) (Hofmeister, Wagoner, & Goodman, 2013).

The paper (Vogl, Weiss, & Donmez, 2014) conducted a detailed review of existing standards that were designed to help guide implementation of PHM in manufacturing. Specifically, many of the current PHM standards were developed within the International Organization for Standardization (ISO) and focus primarily on condition monitoring and diagnostics (ISO, 2002) (ISO, 2003) (ISO, 2012). Few standards include discussion of prognostics (ISO, 2004). The standards review highlighted that only very specific processes benefited from these standards; they are not considered broadly applicable. This study highlights a gap in that no standards are currently available that are both robust and flexible to address the diverse and dynamic environments presented by Smart Manufacturing.

Smart Manufacturing presents a paradigm shift in that manufacturers are thinking differently about how they implement their production technologies, tools, and teams. The field of robotics has already released and is actively working towards a next generation of new products, bolstered by developments in low-level controllers such as proximity detection, image processing, and precise human-safe actuators. In addition, collaborative robotics systems are emerging, enabling robots to work side-by-side with humans and other robots without requiring physical safety barriers. Collaborative robotics are characterized by:

1. Lower total implementation costs
2. Reduced barrier-to-entry in the form of operational technical skill
3. Improved efficiencies and overall equipment effectiveness (OEE) as discussed in (Jeong & Phillips, 2001)
4. Flexible spatial feasibility and responsive configurations
5. Increased safety features allowing humans to work alongside them

For many small and medium-sized manufacturers, the cost of integrating a robot into a historically manual process is the most prohibitive barrier to automation. While the purchase price of a robot is sometimes significant, it is dwarfed by the cost of process integration, programming, and support. Many collaborative robot technologies effectively reduce the overhead associated with safety, programming, and factory floor real estate. As such, the promise of reduced cost and ease of use are seen as a means by which even small and medium-sized enterprises may access and adopt automation technologies (Marvel, 2014).

However, with safety being the principal focus for the current development of collaborative technologies, system performance and reliability have yet to be verified. As such, these systems require the means by which end users can guarantee the application performance, and ultimately establish confidence in the systems on which they will rely. Proper health monitoring and prognostics modeling of system and process performance, in particular, will provide end users with the necessary insights into the reliability of such emerging smart manufacturing technologies.

With this profound interest for installing robotic and other automated platforms, it is increasingly important to create the high-level control strategies necessary for operating them. The competitive landscape has changed the way corporations manage their supply chain solutions. A plant manager cannot lead his or her world class facility with only reactive maintenance systems in place. Rather, PHM based techniques could be seen as a corollary to the cultural principles established in Total Productive Maintenance (TPM) (Nakajima, 1988) and Lean Manufacturing (Shah & Ward, 2003).

3. THE INDUSTRY-INSPIRED USE-CASE

For our use-case, we have created a scenario with two robots collaborating together to accomplish a task in a work cell that is assumed to be a part of an entire production line. The task to be completed can be subdivided into a pick and place operation combined with a drilling operation, as seen later in Figure 3. The pick and place will be performed by a robot which we will name “Ben”. The drilling operation is performed by a robot named “Mike”.

Boxes are generated according to a predetermined cycle time, arriving from an upstream work cell and appearing on a conveyor in front of Ben. Ben picks up a single box after it has been detected, rotates his torso actuators ninety degrees, and places it on a second conveyor that is elevated off the factory floor. Boxes then continue their conveyance route, already facing the correct orientation to receive the drilling operation. When a box is detected in front of Mike, the end effector is extended, grabs the box, drills a hole, and retracts the arm.

We will engage the use case to show the many motion trajectories that could be employed to accomplish this specific work cell’s task. It is an exciting contribution of the work to introduce the notion that we can generate redundant motion sequences to be leveraged for PHM. These will later be identified by the novel monitoring methodology achieved by a formalized separation between the overall system task and the single strategy employed at any one point in time.

It should be noted the use-case assumes a dynamic model of wear that shows increases in wear over time as the number of movements increase in the robot. We are also using a discrete transition system model of each robot's behavior and capabilities.

4. AN LTL-BASED MONITORING SIMULATOR FOR THE INDUSTRIAL USE-CASE

We will now review the individual components of the software simulator framework as implemented on the industry inspired use case. This includes the representation of the involved robot subsystems as discrete transition systems. Further, we explain the linear temporal logic based high level objective description and monitoring.

4.1. Transition System Representation

The two robots in our use case are represented in the form of discrete transition systems. A discrete transition system is a well known concept in Computer Science where it is extensively used in formal proofs for different algorithms and software. For our case, we have also incorporated a continuous state variable in the respective transition systems for representing the wear in the robots. The transition systems of the robots for the industry inspired use-case are given in the Fig. 1. Using notation described in (LaViers, Chen, Belta, & Egerstedt, 2011), for the two robots this representation is given as:

$$T_1 = (\mathcal{Q}_1, q_{0_1}, \rightarrow_1, \Pi_1, h_1, C_1, w_1), \tag{1}$$

$$T_2 = (\mathcal{Q}_2, q_{0_2}, \rightarrow_2, \Pi_2, h_2, C_2, w_2), \tag{2}$$

T_1 represents transition system for Mike and T_2 represents transition system for Ben where

(i) $\mathcal{Q}_1 = \{q^1_1, q^1_2, q^1_3, q^1_4\}$ is the finite set of Mike's states, either hand labeled by a user or generated automatically through a segmentation framework. $\mathcal{Q}_2 = \{q^2_1, \ldots, q^2_8, q^2_9\}$ is the similar set of Ben's states. Superscripts indicate the robot (1 is for Mike, 2 is for Ben).

(ii) q_{0_1} and q_{0_2} are the initial states of Mike and Ben respectively;

(iii) $\rightarrow_i \subseteq \mathcal{Q}_i \times \mathcal{Q}_i$ is a reflexive transition relation of Mike (if $i = 1$) or Ben (if $i = 2$) , where each state has a self-loop, allowing for one robot to transition to a new state without that requirement being imposed on the other robot;

(iv) $\Pi_1 = \{M_{initial}, M_{opengrip}, M_{detect}, M_{drillready}, M_{drill}, M_{closedgrip}\}$ is a finite set of atomic propositions for robot Mike.
Similarly, $\Pi_2 = \{B_{initial}, B_{opengrip}, B_{Detect}, B_{Drop}, B_{grabReady}, B_{Grab}, B_{hold}, B_{IntermedPos}, B_{DropReady}\}$ is a finite set of propositions for Ben.
These propositions represent the status of different subtasks performed by Mike and Ben respectively;

(v) $h_i : \mathcal{Q}_i \mapsto 2^{\Pi_i}$ is a satisfaction (output) map, where state q^i_j satisfies the set $h_i(q^i_j)$ of propositions from Π_i. 2^{Π_i} represents a set of all possible combinations of propositions of one robot. Thus, h_i is a mapping of these combinations to each one of the states in the robot i. It can be seen in Fig. 1 how each of the states has a combination of individual propositions;

(vii) C_1 and C_2 are sets of pairs of the form $(f(x,t), \tau)$. For C_1 we have $(f^1_1(x,t), \tau^1_1)$,...,$(f_{n \times r \times e}(x,t), \tau_{n \times r \times e})$ such that $f^1_j(x,t)$ represents dynamics of a continuous parameter for duration of τ^1_j. In the final pair, $n = 6$ and defines the number of degrees of freedom in Mike; $r = 13$ and is the number of motion primitives in Mike; $e = 2$ representing the two environmental cases e.g., loaded and unloaded condition, for Mike. Similarly for C_2 we have $(f^2_1(x,t), \tau^2_1)$,...,$(f^2_{9 \times 13 \times 2}(x,t), \tau^2_{9 \times 13 \times 2})$;

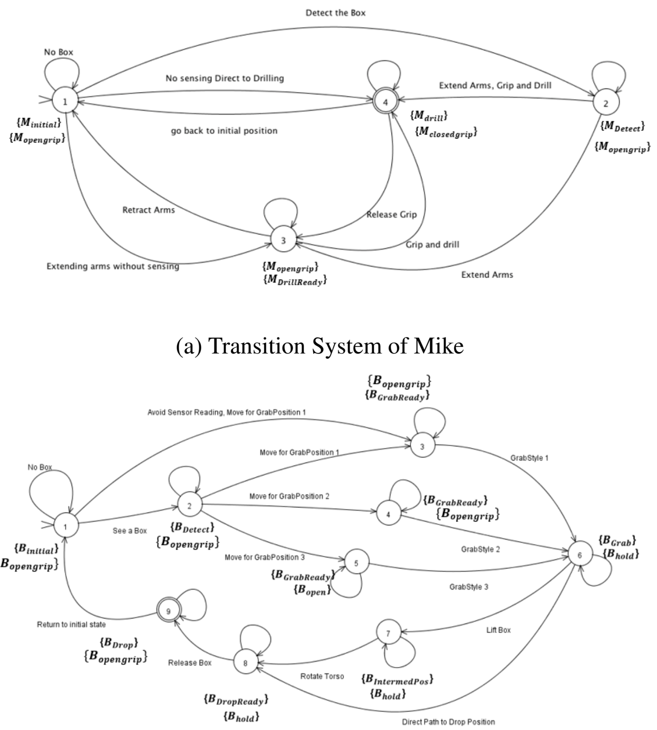
(vi) $w_1 : \rightarrow_1 \mapsto C_1$ and $w_2 : \rightarrow_2 \mapsto C_2$. w_1 and w_2 are mapping from each transition for a respective robot to a pair in corresponding C_1 and C_2. More simply, it is a function that maps all the transitions of a robot to a corresponding wear dynamic.

The states correspond to the robot states while performing the tasks. For example, a state can be the idle state when the robot is waiting for the sensor to detect the box in front of it. The atomic propositions represent statements about the states of the robot and they can be either true or false. The linear temporal logic (LTL) specifications, as will be explained in the next subsection, are described in terms of these statements and the system evolves in terms of them.

The next task is to combine the representation of different robots to describe the whole system in terms of a single transition system. This can be achieved using the composition of the two transition systems. This composition is achieved by taking synchronous product of the transition systems for the individual robots.

The synchronous product of two transition systems T_1 and T_2, denoted as $T_p = T_1 \otimes T_2$, is a new transition system with $(\mathcal{Q}_P, q_{0_P}, \rightarrow_P, \Pi_P, h_P)$. The states are Cartesian pairs of the single robot states, i.e., $\mathcal{Q}_P \subseteq \mathcal{Q}_1 \times \mathcal{Q}_2$, likewise $q_{0_P} = (q_{0_1}, q_{0_2})$. Transitions exist between these joint states if and only if a transition existed between both single states, i.e., $\rightarrow_P \subseteq \mathcal{Q}_P \times \mathcal{Q}_P$ is defined by $(q, q') \in \rightarrow_P$ if and only if $q \neq q'$, $(q_1, q'_1) \in \rightarrow_1$ and $(q_2, q'_2) \in \rightarrow_2$, where $q = (q_1, q_2)$ and $q' = (q'_1, q'_2)$. The set containing atomic propositions for the composition of the two transition systems, denoted as Π_P, is a union of the individual sets of propositions for the two robots that extends to include propositions which apply to situations where both robots are active.

Now we have the transition system for the two robots defined.



(a) Transition System of Mike

(b) Transition System of Ben

Figure 1. Transition Systems of the Robots.

With a formal representation of the robots, we can now define high level tasks for the robots in terms of the states. This is accomplished with LTL specifications and their representation in the form of Büchi automaton. Next we describe the LTL based specifications.

4.2. Linear Temporal Logic (LTL) Specifications

What we want is a tailored transition system according to the high level objectives. This is where the LTL specifications come in. A brief introduction of the LTL operators is given as follows:

LTL formulas are described in terms of the set Π of atomic propositions. LTL specifications describe the high level objectives in the form of Boolean and temporal operators. The Boolean logic operators, that have been used, include, $\neg$ (negation), $\vee$ (disjunction), $\wedge$ (conjunction), and $\rightarrow$ (implication). The temporal operators include, $\mathbf{X}$ (next), $\mathcal{U}$ (until), $\mathbf{F}$ (eventually), and $\mathbf{G}$ (always). LTL formulas are defined over infinite words generated by the transition systems. In particular, the LTL specifications we define, describe the possible actions of our system of robots, $\mathcal{T}_p$.

An LTL formula ϕ is said to satisfy a word of the transition system if the formula ϕ is true for the first position of the word; $\mathbf{X}\phi$ states that at the next state, an LTL formula ϕ is true; $\mathbf{F}\phi$ means that the LTL formula ϕ eventually becomes true at some position of the word; $\mathbf{G}\phi$ means that the LTL formula ϕ is true for all the positions of the word; $\phi_1\ \mathcal{U}\phi_2$ means ϕ_2 eventually becomes true at some position in the word and ϕ_1 is true until that position of the word comes. More complex and sophisticated specifications can be designed using a combination of Boolean and temporal operators. For details (Clarke, Peled, & Grumberg, 1999) can be consulted.

As an example, some high level objectives and their LTL representations are given below. We will only show the basic LTL form $\mathbf{G}(Proposition_1 \rightarrow Proposition_2)$, as this will be the most common form used in practice by manufacturers in specifying their high level objectives.

(i) Ben! Stay in initial position when Mike is performing drilling
$\mathbf{G}\ (M_{drill} \rightarrow B_{initial})$

(ii) Mike! do not grip unless you are in the drilling position
$\mathbf{G}\ (M_{closedgrip} \rightarrow M_{drill})$

(iii) Ben! do not open your hand while you are holding the box
$\mathbf{G}\ (\neg B_{hold} \rightarrow B_{open})$

(iv) Mike! Stay in initial position when Ben is dropping the box
$\mathbf{G}\ (B_{Drop} \rightarrow M_{initial})$

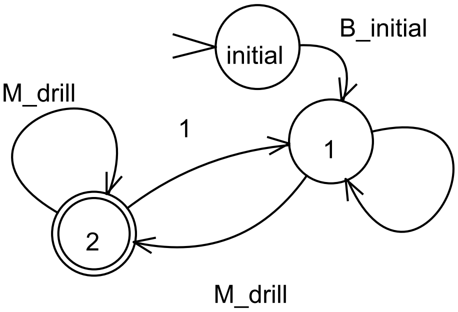


Figure 2. Büchi Automaton representation of an LTL specification

To check whether all words of the transition system, T_p, satisfy an LTL formula ϕ over the set of propositions Π_P, we need to have Büchi Automaton that accepts only the words satisfying ϕ. By the help of a tool, LTL2BA (Gastin & Oddoux, 2001), we are able to get a Büchi Automaton $\mathcal{B}_\phi$ from the LTL specification ϕ. For example, the first specification can be given in the Büchi Automaton form as pictured in Fig. 2.

A tailored representation of the system can then be had by taking a product of the system transition system T_p and $\mathcal{B}_\phi$ to get the final automaton $\mathcal{A}$. Now this automaton as mentioned earlier represents all the *allowed* transitions between states of the system in light of the specifications defined in ϕ. The

LTL specifications are defined in such a way that they define the desired behavior of the whole system. We monitor the behavior of the system by monitoring the transitions in the system. If an error occurs, because of a sensor failure, robot motor failure etc., these specifications are not satisfied and the monitoring system returns a sequence that is **not** satisfied by $T_P \times \mathcal{B}_\phi$. We monitor and verify the desired movements of the robots based on the allowed transitions by using an interface between MATLAB and VREP.

5. APPLICATIONS TO PHM

Through the use of LTL we are able to build the discrete sensor oriented piece of the monitoring scheme. The transition system's representation of the continuous parameter for each robot, C_1 and C_2, allows us to track differential wear functions over time. The two of these combine to create the complete system monitor for use in PHM.

5.1. Results of the LTL-Based Monitor

Figure 3 depicts the three dimensional model of the robotic work-cell in the VREP simulation environment. Figure 4 shows the MATLAB interface displaying continuous time wear parameters and the cycle time associated with the two robots along with the discrete system information. In the top figure, continuous information for the whole system has been presented. This includes wear information of all the joints of the robots according to the dynamic functions defined in the previous section. For each of the robots, wear has been computed for all of the six joints. It can be observed that wear curves for robot Ben are more evenly spread on to all the joints. In comparison, wear curves for robot Mike are mostly defined by joint 6. The third graph in Figure 4(a) represents the cycle time for each task that Mike and Ben are performing.

Figure 4(b) conveys information of the system's discrete nature. The *Motion Primitives* section indicates the current motion primitive of Ben and Mike by filling the corresponding circle for the motion primitive. *Discrete Objective* states the high level overall objective of the system. *Overall Status* indicates if the high level objective specifications are *satisfied* or *violated* by toggling the color of the corresponding bubble.

A generalizable structure of the work is defined by Figure 5. The figure is specifically for the use-case where we have two robots that collaborate with each other, but could be extended to include any number of Robotic Transition Systems. The Robotic Transition Systems, which abstract the physical robots present on the factory floor, are subsequently transformed into the overall Manufacturing System Automaton. The plant maintenance team or robotics engineers create the high-level LTL specifications to monitor the discrete exceptions of the Manufacturing System, which is then mathematically written as the Büchi Automaton of the LTL Spec. The LTL Spec and Manufacturing System Automaton can then be represented in the same automaton, which finally becomes the Discrete System Monitor for PHM applications. The actuator wear is also projected for each joint with respect to the robotic systems to monitor continuous parameters. Discrete and Continuous Prognostic Indicators are finally realized, which is exemplified by the MATLAB interface in Figure 4.

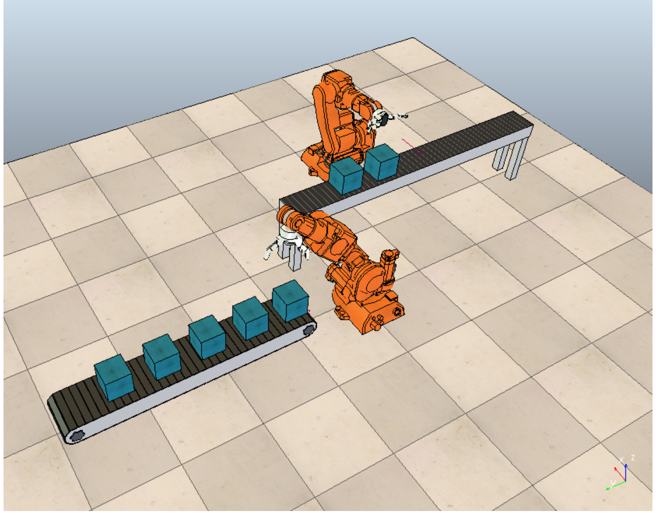
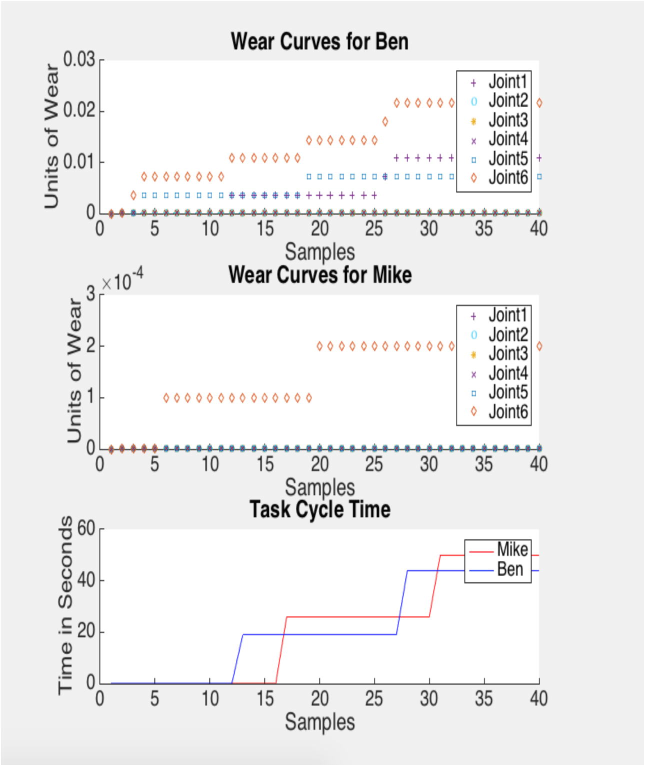


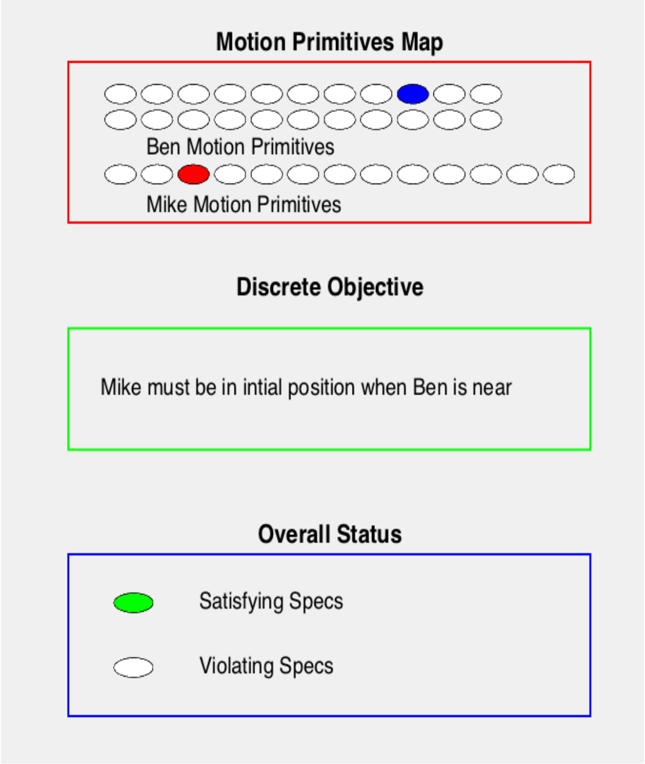
Figure 3. VREP simulation environment of the use case complete with two robots performing the pick and place of the box and subsequent drilling operation.

5.2. Application to Adaptive Multi-Scale PHM

As previously stated, this paper is a part of a larger effort to create an adaptive multi-scale PHM scheme described in (Choo, Beling, LaViers, Marvel, & Weiss, 2015). Adaptive multi-scale prognostics and health management (AM-PHM) is a methodology designed to support PHM in smart manufacturing systems. AM-PHM is characterized by its incorporation of multi-level, hierarchical relationships and PHM information. AM-PHM utilizes diagnostic and prognostic information regarding the current health of the system and constituent components, and propagates it up the hierarchical structure. By doing so, the AM-PHM methodology creates actionable prognostic and diagnostic information along the manufacturing process hierarchy. This information includes the predicted health state upon completion of a task. The health estimates that flow up the hierarchy are based upon simulated operational directives that flow down it. Nodes at given levels along the system hierarchy consume operational profiles from adjacent, higher level nodes. These profiles describe the production goals under consideration by the decision makers (e.g., operators and supervisors) in the superior level. In addition to the traditional workload, bill of materials, and requirements of the manufacturing process, the operational profile may have a focused objective such as minimizing cost or maximizing reliability. Each AM-PHM mod-



(a) Continuous wear information for each robot, Ben and Mike, and their respective task cycle times



(b) Discrete information showing the active motion primitives, current system objective, and a status indicator showing if the high level objective is currently satisfied.

Figure 4. MATLAB interfaces for the continuous and discrete pieces of the monitoring framework

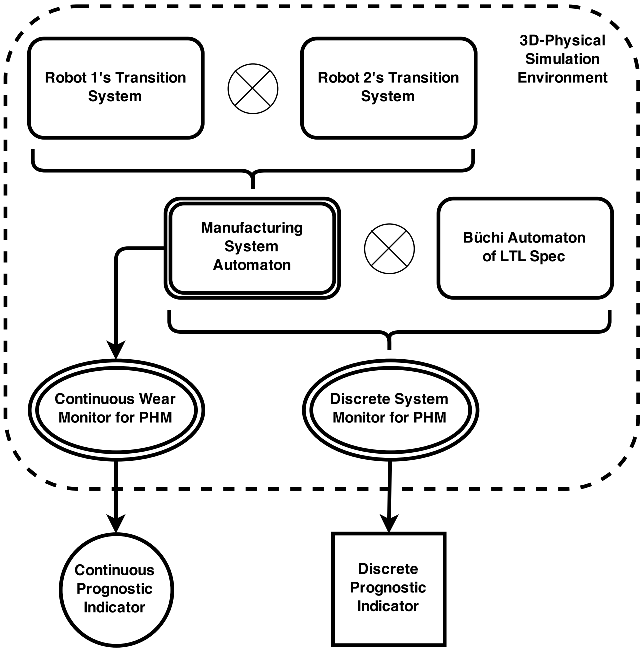

Robot 1's Transition System
Robot 2's Transition System
3D-Physical Simulation Environment
Manufacturing System Automaton
Büchi Automaton of LTL Spec
Continuous Wear Monitor for PHM
Discrete System Monitor for PHM
Continuous Prognostic Indicator
Discrete Prognostic Indicator

Figure 5. A more general representation of the LTL based monitoring system applied to the use-case where two robots are working together to accomplish a task.

ule creates operational profiles for its subordinate AM-PHM modules while producing diagnostic and prognostic information for its higher level subsystem.

The simulator framework described in this paper would provide the capability to estimate wear and other measures of system health with respect to given operational profiles, and so could be the basis for upward push of prognostics and health estimates. In an attempt to deliver true adaptable and scalable information for translating operational profiles into operational directives, LTL specifications can be hierarchical in nature to capture subtopic levels, or the individual motors, and head topic levels, which is the team process flow.

6. CONCLUSION

The paradigm shift in Advanced Manufacturing, where manufacturers are introducing the next generation of flexible and collaborative robotics, has the potential to further shape the sector. This shift, along with Prognostic and Health Management techniques, is a large part of what will enable Smart Manufacturing Systems. The novel LTL-based monitor reviewed in this work introduces a method for connecting continuous and discrete prognostics, and is immediately applicable to the robotic platforms that manufacturers seek to install in their factories.

We have applied this monitor to an industry-inspired use-case and showed in a three dimensional simulation environment how the methodology can be integrated on a robotic workcell. The differential wear functions can be installed to fit the manufacturer specific application, and handled by the automated computing environment for generating wear diagnostics. Intuitive high-level specifications can be applied by systems integrators or plant supervisors for filtering out discrete exceptions. This is especially important as production lines in the advanced manufacturing setting employ an increasing suite of sensors to observe their processes.

Therefore, we have laid the ground work for building intelligent control strategies to evenly spread wear of robotic platforms, ergo maximizing the life of the system. Future work will leverage the supervisory control and model checking found in the monitor to define the multiple ways motions can be performed, and then switch between styles of motion to best extend asset life. This automated flexibility continues to close the gap on waste, both in the form of time and capital expenditure.

The LTL-monitor serves as a blueprint for implementing PHM in robotics and all other forms of automation. The protocols can be written to allow for information flow into the larger supply chain systems scheme, further bolstering the Adaptive, Multi-scale PHM environment. The overall vision gives plant leadership teams and operations management alike the structure to seamlessly integrate their manufacturing capabilities with market demand. As pressures for profitability continue, this will undoubtedly be of interest to industry to ensure productivity, quality, and safety goals.

ACKNOWLEDGMENT

This research is supported by the National Institute of Standards and Technology. We would also like to thank the various industry partners whose support of our research proved invaluable.

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

REFERENCES

Ahmad, R., & Kamaruddin, S. (2012). An overview of time-based and condition-based maintenance in industrial application. *Computers & Industrial Engineering*, *63*(1), 135–149.

Al-Habaibeh, A., & Gindy, N. (2000). A new approach for systematic design of condition monitoring systems for milling processes. *Journal of Materials Processing Technology*, *107*(1), 243–251.

Altintas, Y., Verl, A., Brecher, C., Uriarte, L., & Pritschow, G. (2011). Machine tool feed drives. *CIRP Annals-Manufacturing Technology*, *60*(2), 779–796.

Anderson, A. (2011). Report to the president on ensuring american leadership in advanced manufacturing. *Executive Office of the President*.

Barajas, L. G., & Srinivasa, N. (2008). Real-time diagnostics, prognostics and health management for large-scale manufacturing maintenance systems. In *Asme 2008 international manufacturing science and engineering conference collocated with the 3rd jsme/asme international conference on materials and processing* (pp. 85–94).

Batzel, T. D., & Swanson, D. C. (2009). Prognostic health management of aircraft power generators. *Aerospace and Electronic Systems, IEEE Transactions on*, *45*(2), 473–482.

Biehl, S., Staufenbiel, S., Recknagel, S., Denkena, B., & Bertram, O. (n.d.). Thin film sensors for condition monitoring in ball screw drives.

Borisov, O., Fletcher, S., Longstaff, A., & Myers, A. (2013). New low cost sensing head and taut wire method for automated straightness measurement of machine tool axes. *Optics and lasers in engineering*, *51*(8), 978–985.

Choo, B., Beling, P. A., LaViers, A. E., Marvel, J. A., & Weiss, B. A. (2015). Adaptive Multi-scale PHM for Robotic Assembly Processes. *Annual Conference of the PHM Society*(In review).

Clarke, E. M. M., Peled, D., & Grumberg, O. (1999). *Model checking*. MIT Press.

Datta, K., Jize, N., Maclise, D., & Goggin, D. (2004). An ivhm systems analysis & optimization process. In *Aerospace conference, 2004. proceedings. 2004 ieee* (Vol. 6, pp. 3706–3716).

Gastin, P., & Oddoux, D. (2001, July). Fast LTL to Büchi automata translation. In G. Berry, H. Comon, & A. Finkel (Eds.), *Proceedings of the 13th International Conference on Computer Aided Verification (CAV'01)* (Vol. 2102, p. 53-65). Paris, France: Springer.

Haimes, Y. Y. (2005). *Risk modeling, assessment, and management* (Vol. 40). John Wiley & Sons.

Haimes, Y. Y. (2012). Systems-based guiding principles for risk modeling, planning, assessment, management, and communication. *Risk Analysis*, *32*(9), 1451–1467.

Hofmeister, J., Wagoner, R., & Goodman, D. (2013). Prognostic health management (phm) of electrical systems using conditioned-based data for anomaly and prognostic reasoning. *Chemical Engineering Transactions*, *33*, 991-996.

Holland, S., Barajas, L., Salman, M., & Zhang, Y. (2010). PHM for Automotive Manufacturing and Vehicle Applications. *Annual Prognostics and Health Management Conference*.

Hu, S. J., & Koren, Y. (1997). Stream-of-variation theory for automotive body assembly. *CIRP Annals-Manufacturing Technology*, *46*(1), 1–6.

Huzaifa, Umer and Marvel, Jeremy A. and LaViers, Amy E. (2015). Incorporating Continuous System Parameters in an LTL-based Monitoring Scheme. *Unpublished*.

ISO. (2002). *Condition monitoring and diagnostics of machines vibration condition monitoring part 1: General procedures* (Tech. Rep. No. ISO 13373-1). International Organization for Standardization.

ISO. (2003). *Condition monitoring and diagnostics of machines data processing, communication and presentation part 1: General guidelines* (Tech. Rep. No. ISO 13374-1). International Organization for Standardization.

ISO. (2004). *Condition monitoring and diagnostics of machines, prognostics part 1: General guidelines* (Vol. ISO/IEC Directives Part 2; Tech. Rep. No. ISO13381-1). International Organization for Standardization.

ISO. (2012). *Condition monitoring and diagnostics of machines vocabulary* (Tech. Rep. No. ISO 13372). International Organization for Standardization.

Jeong, K.-Y., & Phillips, D. T. (2001). Operational efficiency and effectiveness measurement. *International Journal of Operations & Production Management*, *21*(11), 1404–1416.

LaViers, A., Chen, Y., Belta, C., & Egerstedt, M. (2011). Automatic sequencing of ballet poses. *Robotics & Automation Magazine, IEEE*, *18*(3), 87–95.

Marvel, J. A. (2014). *Collaborative robots: A gateway into factory automation.* Retrieved from `thomasnet.com`

Nakajima, S. (1988). Introduction to TPM: total productive maintenance. *Productivity Press, Inc, P. O. Box 3007, Cambridge, Massachusetts 02140, USA, 1988. 129*.

Peng, Y., Dong, M., & Zuo, M. J. (2010). Current status of machine prognostics in condition-based maintenance: a review. *The International Journal of Advanced Manufacturing Technology*, *50*(1-4), 297–313.

Shah, R., & Ward, P. T. (2003). Lean manufacturing: context, practice bundles, and performance. *Journal of operations management*, *21*(2), 129–149.

Shen, T., Wan, F., Cui, W., & Song, B. (2010). Application of prognostic and health management technology on aircraft fuel system. In *Prognostics and health management conference, 2010* (pp. 1–7).

Vogl, G. W., Weiss, B. A., & Donmez, M. A. (2014). Standards for Prognostics and Health Management (PHM) Techniques within Manufacturing Operations. *Annual Conference of the PHM Society*.

BIOGRAPHIES

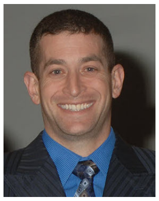
Gerald Heddy is a M.S. student in the Department of Systems and Information Engineering at the University of Virginia. His research interests lie in the field of Robotics as applied to the Advanced Manufacturing sector and Smart Manufacturing Systems. Prior to UVa, he received his B.S. from Lehigh University in Industrial Engineering and worked in manufacturing at The Hershey Company as a Business Unit Team Leader.

Umer Huzaifa is a Ph.D. student in the Department of Systems and Information Engineering at the University of Virginia. He holds a B.S. degree in Electrical Engineering from University of Pakistan. He has a background in Electrical Engineering with a focus on control systems and robotics. His research interests lie in the field of supervisory control and hybrid systems. Specifically, he is focused on developing mathematical tools for complex motion planning of mobile robots.

Dr. Peter A. Beling is an associate professor in the Department of Systems and Information Engineering at the University of Virginia. Dr. Beling received his Ph.D. in Operations Research from the University of California at Berkeley. Dr. Belings research interests are in the area of decision-making in complex systems, with emphasis on adaptive decision support systems and on model-based approaches to system-of-systems design and assessment. His research has found application in a variety of domains, including prognostics and health management, mission-focused cybersecurity, and financial decision-making.

Dr. Yacov Haimes is the Lawrence R. Quarles Professor of Systems and Information Engineering, Civil and Environmental Engineering, and Founding Director (1987) of the Center for Risk Management of Engineering Systems at the University of Virginia. He received his M.S. and Ph.D. (with Distinction) degrees in Systems Engineering from UCLA, and his B.S. degree in Mathematics, Physics, and Chemistry from the Hebrew University, Jerusalem. On the faculty of Case Western Reserve University (1970-1987), he chaired the Systems Engineering Department. As an American Association for the Advancement of Science-American Geophysical Union Congressional Science Fellow (1977-78), Dr. Haimes served in the Office of Science and Technology Policy, Executive Office of the President, and on the United States House of Representatives Science and Technology Committee. From 1990 to 2011 he served as a consultant to the Software Engineering Institute, Carnegie Mellon University, and for the last decade as a visiting scientist. He is a Fellow of seven societies: ASCE, IEEE, INCOSE, AWRA, IWRA, AAAS, and Society for Risk Analysis (SRA), (where he is a past President). The Fourth Edition of his most recent book, Risk Modeling, Assessment, and Management, will be published by Wiley and Sons in February 2015 (the first three editions were published in 1998, 2004 and 2009). Professor Haimes is the recipient of the 2014 ASCE American Academy of Water Resources Engineers Founders Award; the 2010 Distinguished Educator Award presented by SRA; the 2007 Icko Iben Award presented by AWRA; the 2001 Norbert Weiner Award, presented by IEEE-SMC; the 2000 Distinguished Achievement Award, presented by SRA; the 1997 Warren A. Hall Medal, the highest award presented by Universities Council on Water Resources; the 1995 Georg Cantor Award, presented by the International Society on Multiple Criteria Decision Making, and the 1994 Outstanding Contribution Award presented by the IEEE-SMC; following Hurricane Katrina, he was appointed as the 2007 Arthur Maass-Gilbert White Fellow under the U.S Army Corps of Engineers, Institute for Water Resources (IWR), among others. He is a registered Professional Engineer in Ohio and Virginia; Diplomate of the American Academy of Water Resources Engineers (and a Founding Trustee of the AAWRE); the Past Engineering Area Editor of Risk Analysis: An International Journal. He has authored (and co-authored) six books and 300 technical publications, over 200 of which were published in archival-refereed journals. He has served as dissertation/thesis advisor to 38 Ph.D. and over 80 M.S. students.

Dr. Jeremy Marvel is a project leader and research scientist in the Intelligent Systems Division of the National Institute of Standards and Technology (NIST) in Gaithersburg, MD. Dr. Marvel received his Ph.D. in 2010 in computer engineering from Case Western Reserve University in Cleveland, OH. Since joining the research staff at NIST, he has established the Collaborative Robotics Laboratory, which is engaged in research dedicated to developing test methods and metrics for the performance and safety assessments of collaborative robotic technologies. His research focuses on intelligent and adaptive solutions for robot applications, with particular attention paid to human-robot collaborations, multi-robot coordination, safety, perception, self-guided learning, and automated parameter optimization. Jeremy is currently engaged in developing measurement science methods and artifacts for the integration and application of robots in collaborative assembly tasks for manufacturing.



Dr. Brian A. Weiss has a B.S. in Mechanical Engineering (2000), Professional Masters in Engineering (2003), and Ph.D. in Mechanical Engineering (2012) from the University of Maryland, College Park, Maryland, USA. He is currently the Associate Program Manager of the Smart Manufacturing Operations Planning and Control program and the Project Leader of the Prognostics and Health Management for Smart Manufacturing Systems project within the Engineering Laboratory (EL) at the National Institute of Standards and Technology (NIST). Prior to his leadership roles in the SMOPAC program and the PHM4SMS project, he spent 15 years conducting performance assessments across numerous military and first response technologies including autonomous unmanned ground vehicles; tactical applications operating on Android devices; advanced soldier sensor technologies; free-form, two-way, speech-to-speech translation devices for tactical use; urban search and rescue robots; and bomb disposal robots. His efforts have earned him numerous awards including a Department of Commerce Gold Medal (2013), Silver Medal (2011), Bronze Medals (2004 and 2008), and the Jacob Rabinow Applied Research Award (2006).

Dr. Amy LaViers is an Assistant Professor in Systems and Information Engineering and Director of the Robotics, Automation, and Dance Lab at the University of Virginia. She aims to extract useful features from human movement for robotic applications, such as, endowing co-robots the ability to work alongside human workers in manufacturing plants. She also works to classify organized human movement, such as, providing quantitative comparison between genres of movement styles. Her research began at Princeton University where she earned a certificate in Dance and B.S.E. in Mechanical and Aerospace Engineering. She went on to complete a M.S. and Ph.D. in Electrical and Computer Engineering at the Georgia Institute of Technology. She is currently enrolled in the Laban/Bartenieff Institute for Movement Studies Certification in Movement Analysis (CMA) Modular program.

Proceedings of the ASME 2016 International Design Engineering Technical Conferences &
Computers and Information in Engineering Conference
IDETC/CIE 2016
August 21-24, 2016, Charlotte, North Carolina

IDETC2016-59721

ENABLING SMART MANUFACTURING TECHNOLOGIES FOR DECISION-MAKING SUPPORT

Moneer Helu
National Institute of Standards and Technology
Gaithersburg, Maryland, USA

Don Libes
National Institute of Standards and Technology
Gaithersburg, Maryland, USA

Joshua Lubell
National Institute of Standards and Technology
Gaithersburg, Maryland, USA

Kevin Lyons
National Institute of Standards and Technology
Gaithersburg, Maryland, USA

KC Morris
National Institute of Standards and Technology
Gaithersburg, Maryland, USA

ABSTRACT

Smart manufacturing combines advanced manufacturing capabilities and digital technologies throughout the product lifecycle. These technologies can provide decision-making support to manufacturers through improved monitoring, analysis, modeling, and simulation that generate more and better intelligence about manufacturing systems. However, challenges and barriers have impeded the adoption of smart manufacturing technologies. To begin to address this need, this paper defines requirements for data-driven decision making in manufacturing based on a generalized description of decision making. Using these requirements, we then focus on identifying key barriers that prevent the development and use of data-driven decision making in industry as well as examples of technologies and standards that have the potential to overcome these barriers. The goal of this research is to promote a common understanding among the manufacturing community that can enable standardization efforts and innovation needed to continue adoption and use of smart manufacturing technologies.

Keywords: Smart manufacturing, Data-driven decision making, Standardization, Systems integration

INTRODUCTION

Manufacturing has increasingly relied on software systems to improve productivity and manage operations. Modern manufacturing equipment can often support networking and monitoring as well as reporting performance metrics to varying degrees. Even older, legacy equipment can be retrofitted to provide similar capabilities. New technologies have been proposed to enable better performance monitoring and control for manufacturing systems, including visualization tools and advanced analytical capabilities to support scheduling, performance monitoring, and anomaly detection. Such technologies have been driven by demands for increased flexibility and resource efficiency. Other business drivers include smaller customer orders and tighter delivery dates [1] and greater responsiveness to sustainability concerns [2]. As new capabilities have been introduced into manufacturing systems to respond to these and other technology drivers, more complexity has been added to manufacturing operations, which in turn has forced the use of new and better technologies for system design and management.

The term “smart manufacturing” has been adopted to refer to manufacturing systems that combine advanced manufacturing capabilities and digital technologies throughout the product lifecycle. Such systems are characterized by improvements in the following capabilities [3]:

- Communication with other systems across a network
- Collection and response to operational data
- Support for decision making
- Increased specialization to accommodate advanced materials

Moreover, each component of a smart manufacturing system may contain all of these capabilities for a particular function and thus can be considered a smart manufacturing system in itself.

Smart manufacturing incorporates many of the historical manufacturing paradigms that have been the focus of

Helu, Moneer; Libes, Donald; Lubell, Joshua; Lyons, Kevin; Morris, Katherine.
“Enabling Smart Manufacturing Technologies for Decision-Making Support.”
Paper presented at the ASME Computers and Information in Engineering Conference, Charlotte, NC, Aug 21-Aug 24, 2016.

researchers' and practitioners' efforts to improve manufacturing practices. Examples of these paradigms include lean, flexible, agile, sustainable, digital, and cloud manufacturing. Smart manufacturing can enable aspects of these paradigms for all manufacturers from small businesses to large enterprises [4],[5]. One critical aspect of these systems is the use of data and information to make informed decisions. An example technology area that reflects this characteristic is the Industrial Internet of Things (IIoT) based on the Internet of Things (IoT) concept. In the IoT, many commonly used items are networked and may be equipped with computers capable of collecting and processing data and responding to external events, which essentially makes them "smart." The IIoT extends this idea to manufacturing where the items are the sensors, devices, equipment, and systems found within manufacturing facilities. Thus, whereas the IoT connects mainly consumer devices, the IIoT connects devices typically found in an industrial setting. By networking these items, manufacturers can have access to wide swaths of data and information to support decision making.

There is wide agreement that innovations, such as smart manufacturing and the IIoT, can provide important benefits to manufacturers. For example, an Industry Week survey found that 88% of surveyed manufacturers believe that the IIoT is an important trend and 63% also believe that it is critical to their success [6]. This trend was also found by a recent Accenture survey of manufacturers [7]. However, the majority of respondents – 66% in the Industry Week survey and 71-93% in the Accenture survey – also do not have a specific and comprehensive strategy to deploy and use the technology [6],[7]. A similar industry study from LNS Research found that only 13% of surveyed companies were moving forward with the IIoT today [8], and some industry experts estimate that only 5% of manufacturing machines are currently being digitally monitored [9]. These survey results should come as no surprise given that the IIoT and many smart manufacturing technologies are in the early phases of market adoption where compelling use cases and education are essential for success. The goal of this paper is to begin to meet this need by understanding the requirements for manufacturers to leverage smart manufacturing technology to support decision making.

BACKGROUND

We can think of a general data-driven decision-making process as being composed of seven basic activities that occur once the purpose or goal of the decision is well understood as shown in Figure 1 [10]. The first activity, "Scope," refers to defining the boundaries and key performance indicators (KPIs) and metrics needed to address the goal of the decision. "Identify" determines the data and information needed to support the calculation of KPIs and metrics within the boundaries of analysis. "Collect" requires using tools and methods to gather the identified data and information from the system of interest, while "Transmit" requires using tools and methods to move the collected data and information from the system of interest to where it may be analyzed. "Analyze" is the calculation of the identified KPIs and metrics from the collected data and information using appropriate methodologies. "Share" refers to accessing previously generated data, knowledge, and resources to reduce the cost, expertise, time, and training needed to generate new intelligence through analysis. Finally, "Retrieve" is the storing and accessing of generated intelligence quickly and accurately without losing knowledge to support future decisions.

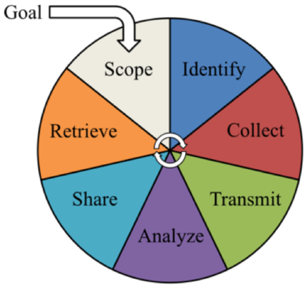


Figure 1: Generalized data-driven decision-making process [10].

One of the primary purposes of much of the smart manufacturing technology on the market is to improve on the general data-driven decision-making process described previously [10]. Enabling technologies and standards have been established to support solutions that help manufacturers use data in new and valuable ways. One example is in the area of process monitoring and control systems, which are widely used throughout manufacturing industries [11]. At the heart of these systems are control-feedback loops. As shown in Figure 2, a control-feedback loop includes the following devices:

- A controlled process; e.g., machining.
- Actuators that act upon the environment; e.g., a pump to deliver coolant to the machine tool frame.
- Sensors that measure physical properties of the process and convert measurements into outputs that a controller can interpret; e.g., a sensor to measure the temperature of the machine tool frame.
- A controller that adjusts actuators based on sensor input; e.g., the controller may activate a coolant pump if the measured temperature of the machine tool frame exceeds a certain value.

The control-feedback mechanism shown in Figure 2 is influenced by disturbances to the process environment as well as by human interaction through a human-machine interface (HMI). In addition, the controller and sensors may receive input from remote diagnostics and maintenance tools.

The devices controlling a process in a smart manufacturing system may also be "smart." For example, a smart sensor has the ability to perform computations on process measurement data before passing the data to the controller. The HMI and diagnostics and maintenance tools may adopt modern information technologies and Internet protocols. As a consequence, today's smart manufacturing systems increasingly resemble traditional IT systems. Hence, they share some of the same potential weaknesses and vulnerabilities.

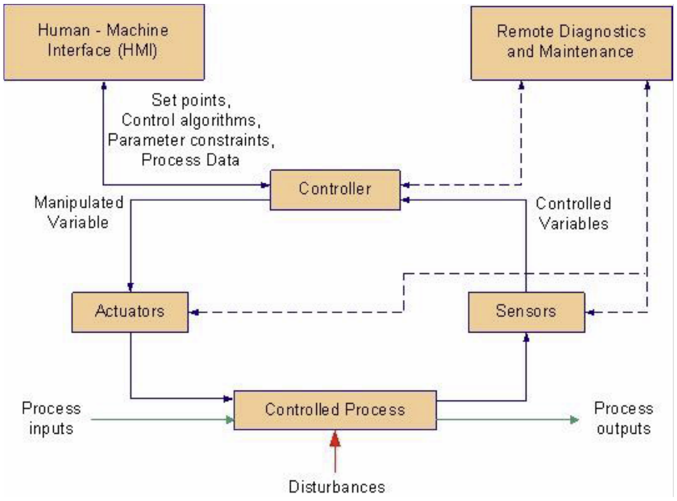

Human - Machine Interface (HMI)
Remote Diagnostics and Maintenance
Set points, Control algorithms, Parameter constraints, Process Data
Controller
Manipulated Variable
Controlled Variables
Actuators
Sensors
Process inputs
Controlled Process
Process outputs
Disturbances

Figure 2: Industrial Control Systems operation [11].

Other examples exist in process monitoring and control. These systems in manufacturing require data interoperability to capture often disparate data and information streams that exist within manufacturing systems. MTConnect is an example of a manufacturing data exchange standard that enables data-driven decision making. It is an open-source standard designed for data and information flowing from shop-floor devices, equipment, and applications [12]. There are several commercial solutions that have been created using the MTConnect standard, such as System Insights VIMANA, TechSolve ShopViz, and FORCAM Force [9],[13]. These and other solutions and standards available to manufacturers have allowed them to monitor shop-floor operations using dashboards that report appropriate KPIs and metrics. Despite the potential value provided by technologies and standards for process monitoring and control and decision making in general, manufacturers remain hesitant to adopt these solutions because of the inherent implementation challenges and potential security liabilities they pose.

Understanding how to integrate and deploy new technology is not trivial for a manufacturer or technology vendor. To benefit from these advances, manufacturers often require technical insight just to navigate the breadth and type of technologies now available to improve their systems [1],[14]. Preliminary technology development and validation also occur in research environments, which may not contain the implementation barriers that often exist in production environments [10]. For example, sensors can operate differently when installed in real production environments and may require interfaces to function with older equipment. Wireless networks may function differently in different environments based on existing sources of interference and the demands placed on the network. In addition, different components of a manufacturing system are connected by a wide range of interfaces with different levels of technological maturity and openness as well as different functional scopes [10].

Collaboration between manufacturers and solution providers will help assure that smart manufacturing technologies work well together. In this way, stakeholders can identify problem areas in deployment that may have been missed when developing smart solutions. Best practices for using solutions can emerge as will opportunities for standards. Additionally, the collective knowledge may expose systemic problems that were not identified in isolated performance testing. The sharing of this expertise can enable successful deployment and more widespread adoption of smart manufacturing technologies and can benefit the entire manufacturing community if made public. Ultimately, pooling the knowledge of many can create a resource that will benefit all and allow the community to discover trends and opportunities that would otherwise be missed.

Helu et al. [10] proposed the development of a collective knowledgebase to identify implementation barriers and solutions for deploying smart manufacturing technology. This paper expands that concept by identifying common activities for and barriers to data-driven decision making in manufacturing. This work forms an outline for when, where, and how new technologies offer the potential to help manufacturers make better decisions. It also provides an initial framework on which to build a base of experience when using these technologies and understanding the risks involved therein.

FRAMEWORK APPROACH

The software community has developed a large body of work that addresses how to assure the performance of software systems. This work serves as a useful template to address performance assurance for data-driven decision making in manufacturing. A foundation for our approach is the Common Weakness Enumeration (CWE). The CWE is based on a model of collaboration where problems with software infrastructures are collected and documented [15]. It is a critical component of a cybersecurity strategy that collects the experience of many software system users and distills learned shortcomings into a form that can benefit others. It categorizes reported issues, tracks the frequency of these issues, and provides documented solutions. The CWE forms a basis for addressing deficiencies in cyberdefense for many organizations.

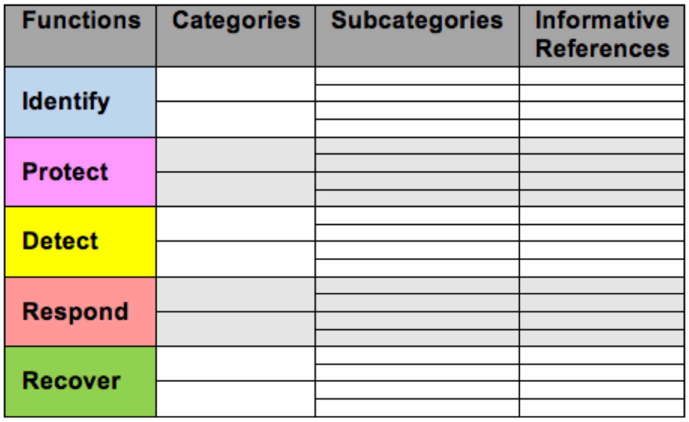
Based on Helu et al. [10], we propose to apply the CWE model of collaborative experience to aid the deployment of smart manufacturing technologies for data-driven decision making. Using collaboration to find and share critical success stories, enable more rapid deployment of the technologies, and identify opportunities for improvements requires an organized means of enumerating common activities for and barriers to data-driven decision making in manufacturing. To organize such an approach and identify relevant content areas, we leverage a similar approach from the security community: the Cybersecurity Framework [17].

As cybersecurity has become an increasingly critical concern, considerable focus has been given to developing a comprehensive set of tools and guidelines that can educate various stakeholders in an organization about the intricacies of cybersecurity. The Cybersecurity Framework is one result of these efforts that was developed for critical infrastructure organizations to better manage and reduce cybersecurity risks [17]. The Cybersecurity Framework provides a way for organizations to describe their current security posture and target state and to communicate and assess progress toward meeting goals. It is organized in a hierarchical fashion, which allows for high-level as well as detailed descriptions of security activities. Thus, the Cybersecurity Framework has a broad base of users. It can facilitate communication not only between different categories of stakeholders but also between different levels of management within an organization, e.g., between a chief executive and cybersecurity professionals responsible for implementation. In addition, the Cybersecurity Framework links desired security outcomes to specific sections of standards, guidelines, and best practices, which offers guidance on how to achieve desired cybersecurity outcomes.

A major component of the Cybersecurity Framework is the Framework Core, which is a taxonomy of cybersecurity activities common across critical infrastructure sectors [17]. The highest level of the Framework Core consists of the following five functions denoting basic cybersecurity activities: Identify, Protect, Detect, Respond, and Recover. Each of these functions is subdivided into categories, which are high-level outcomes tied to a particular requirement or activity. Each category in turn contains a set of subcategories, which are specific lower-level outcomes that support the category's higher-level outcome. Each subcategory points to informative references providing guidance for achieving the subcategory's outcome. Figure 3 provides a high-level structure of the Framework Core.

Because it provides a structure that enables capabilities similar to the ones we are interested in, we adapted the approach of the Cybersecurity Framework when defining the functional areas and categories of activities to be accomplished for data-driven decision making in manufacturing. Two especially attractive capabilities are the utility of the Cybersecurity Framework as a communication tool and its approach of linking goals to actionable guidance. The decision-making process described previously consists of seven functional areas. For each of those areas, we describe the categories of activities and sub-activities required to achieve the function. We also provide examples of the barriers to successful implementation of the listed activities and the enabling solutions that are available to address these barriers. Note that these descriptions are not meant to be exhaustive. They are meant to provide a framework for others to contribute towards a collaborative, community-developed knowledgebase.

In our approach, we take advantage of instances where the requirements of cybersecurity and decision making in manufacturing are well aligned. For example, consider the Framework Core "Identify" function, which has been defined as: "Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities" [17]. This definition is similar to that of the Identify function in our proposed knowledgebase since both involve establishing an understanding of physical and human resources, business environment, capabilities, intellectual property, information, policies, and risk management strategy. Another example is the "Asset Management" category in the Framework Core Identify function. The high-level outcome for this category is defined as: "The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy" [17]. Again, the definition is applicable to both cybersecurity and decision making in manufacturing.



Functions	Categories	Subcategories	Informative References
Identify			
Protect			
Detect			
Respond			
Recover			

Figure 3: Cybersecurity Framework Core [17].

In addition to overlap between the requirements of cybersecurity and decision making in manufacturing, our work relied on literature and industry experience as appropriate to generate a fuller perspective on the requirements and barriers to data-driven decision making in manufacturing. The result of our work was documented in a spreadsheet resource that can serve as the foundation of a larger knowledgebase. The content of this spreadsheet is discussed in the next two sections of this paper.

REQUIREMENTS FOR DECISION MAKING

Deploying data-driven decision-making technologies into manufacturing systems creates a system-of-systems integration challenge. The first and most important step in navigating this challenge is to identify the requirements of the systems through a variety of methods including literature reviews and pilot studies. These requirements serve as a foundation for realizing critical manufacturing needs (current and future) that can be effectively measured and ranked against other drivers. Similar to the Cybersecurity Framework, requirements are understood through the activities that they must support. They are captured within each function as a set of categories of activities which are then broken down into sub-activities as described previously. We can then identify barriers and enabling technologies to accomplish each subactivity listed.

Table 1 provides an example of our approach for one category of activities in the Analyze function: "Select appropriate analysis algorithms to assess data to satisfy the goal of the analysis." This example illustrates the subactivities involved to perform any general manufacturing analysis. Manufacturing analyses are conducted to maintain the efficiency and effectiveness of manufacturing operations and to serve as a foundation for continuous improvement. A critical aspect of manufacturing analysis is the selection of appropriate algorithms

Table 1: Subcategory of activites required to select algorithms for data analysis.

Subcategory of Activities	Barriers to Implementation
Identify algorithms (or describe algorithm requirements if there are no known algorithms)	Explicit cost: Implementations costs money. Implicit cost: Even free implementations can involve expensive installation, maintenance, integration, tracking bug patches, finding support.
	Choices are overwhelming, many algorithms have subtle differences that are not at first important. Algorithms may have different implementations.
Select parameters	May not be possible to identify optimal parameters; Heuristics and/or extensive experimentation likely to be necessary.
Describe time performance requirements	Performance is often hard (or impossible) to quantify; performance may take too long
Describe memory performance requirements	
Describe the uncertainty requirements	Lack of common practices for quantifying manufacturing uncertainty
Describe reliability requirements	Many algorithms trade off reliability for speed as most optimal algorithms are exponential (really, NP-complete).
Determine degree of opacity/transparency (and possibly justify lack thereof)	Some solutions are black boxes. Even ostensibly transparent algorithms (i.e., neural networks) come with no explanation.
Describe extensibility (or lack thereof)	Some algorithms cannot be readily extended.
Identify and justify proprietary, commercial, patented, secret algorithms.	Some algorithms are proprietary, patented, etc. which restrict usage, distribution, etc.
Determine required expertise	Expensive/difficult to find/become expert

and their implementation. Table 1 also inclues the barriers that influence how a company decides on a specific analysis solution. Collecting the information on the different barriers that a manufacturer will face provides an opportunity for understanding and prioritizing the trade-offs that must be balanced, such as cost, data storage, measurement uncertainty, reliability, response time, extensibility, openness, and required expertise. In addition, an understanding of barriers begins the process of identifying solutions. The remainder of this section describes some of the key categories of activities for each of the seven functions that compose data-driven decision making.

Function #1: Scope

The scope sets the stage for establishing or identifying the requirements for a problem space to which smart manufacturing technology will be applied. A properly scoped work effort can ensure a company's success or failure. Too large a scope and the company may never achieve significant progress toward improving its smart manufacturing capabilities while too small a scope may result in mediocre results and poor marks by management. By first determining the appropriate focus, key system requirements, associated technologies, and significant barriers for deploying new technologies, companies can most effectively direct their efforts for maximum impact. Communications has a significant role in how one defines the scope as all manufacturing activities must be coordinated with internal and external stakeholders. This includes issues such as personnel knowing their roles and how to interact and coordinate with stakeholders. The categories of activities involved in setting the scope are as follows:

- Analysis of the scope to understand the business environment, including the organization's mission, objectives, stakeholders, and activities
- Communication with stakeholders to understand interactions and dependencies

Function #2: Identify

Identifying key systems and data is an essential first step for planning and implementing new technologies for smart manufacturing. The requirements should have a direct and defined correlation to the smart manufacturing goals that map to business drivers and support the efforts that will have been made clear in the scoping activities. In this category, one identifies specific analysis needs in terms of manufacturing processes, associated resources, and data sources and flows. The identified processes and data, such as energy and material utilization, will support the goals designated in the scope:

- Manage assets so as to understand the data, people, devices, systems, and facilities involved
- Understand the operational environment, including the material and information flows to and from assets
- Understand data collection capabilities of different assets
- Understand the relationship between scope and data needs
- Specify data collection requirements for specific analysis activities

Function #3: Collect

Data from decision-support and analysis applications, some developed internally and some commercial, need to be collected and key input/output parameters and other relevant information captured. Many newer manufacturing resources now support continuous monitoring, detect and communicate key events, and provide essential and reliable data collection. Older systems can be retrofitted to collect various types of performance information but instructions for doing so do not exist.

Data can be collected for a variety of purposes. For example, detailed data collection may be used for a thorough analysis of a manufacturing process for process improvements. This type of collection may involve modeling the physics of the process and supports offline analysis. The analysis is often relatively complex and requires significant computation. Conversely data can be collected to support real-time control of systems. This type of data collection involves carefully identified performance indicators that can be used to determine a need for adjustments in the system's operation. Frequently, there is a relationship between these two types of data since detailed analysis is often conducted to plan for operational control.

Data can be collected through several means. Reviews of external studies (industry, academia, and government) can be used to collect comparable data sets to those operations within an organizaiton. The most applicable results can be obtained through collecting data internally within the enterprise. Internal data collection is a larger undertaking and is the focus of the activities for this function. Categories of activities in this area include:

- Continuous monitoring
- Detection and communication of performance problems
- Collection methods

Function #4: Transmit

Transmitting data requires the physical movement of data from the data source to the point where the analysis occurs. For example, companies can move data from machine tools on the shop floor to an enterprise database that is accessible to engineers using MTConnect. This supports close to real-time analysis of shop-floor control and performance. Smart manufacturing is prefaced on automated dissemination of data ensuring proper delivery and requires methods beyond the use of portable digital-storage devices, such as thumb-drives. The transmission of data involves activities in a number of areas to ensure that the data arrives where it is needed in a usable and reliable manner. These activities fall into the following categories:

- Data availability and timeliness
- Data integrity in terms of both semantics and completeness
- Data tracability
- Infrastructure maintenance
- Cybersecurity
- Integration into manufacturing operations

Function #5: Analyze

A hallmark of smart manufacturing is that detailed analyses of manufacturing systems are being made more readily available in terms of speed, accuracy, and general accessibility of analysis applications. Categories of activities that support these capabilities include:

- Identification of analysis techniques appropriate to the problem
- Preparation of data for the analysis
- Visualization methods
- Validation and verification

Companies have made great progress in analyzing various aspects of manufacturing to better produce products. Key drivers continue to be cost, on-time product delivery, and asset utilization. Computing power and networking capabilities are making complex analysis using real-time data available for manufacturing systems during operations.

Function #6: Share

Smart manufacturing is defined by the ability to communicate data, information, and knowledge throughout the enterprise. To get maximum utility from an analysis, it is essential that information collected be stored in formats that promote sharing between the company's various analysis applications, between the analysis applications and the operations, and with a variety of stakeholders. For example, planning simulations run by manufacturing engineers will need to send results to the factory floor. The ability to share data provides the opportunity for companies to undertake activities such as storing data and information for reuse, identifying storage technology, and defining resource registries. Categories of activities in this area include:

- Planning for data and content reuse
- Implementing data-sharing environments, including systems, policies, and procedures
- Protecting sharable resources

Function #7: Retrieve

Due to the various types and formats of data being stored, having an optimal way to retrieve the data is important. Retrieval effectiveness will include identifying the right information, withdrawing the data at the right time, and providing it to the right user in the right format for its use. The categories of activities in the retrieve function are:

- Ensuring accessibility of data resources
- Presentation of data
- Search and query of data through formal methods
- Managing traceability of data

Common Requirements and Enabling Technologies

There are a number of requirements and enabling technologies that are common across the seven functions reviewed in this section. These examples reflect the interdependency of the functions and how complementary efforts better ensure that problems be addressed by taking a systems-level perspective. One example area is asset management. This is an important consideration whether tracking manufacturing equipment and tools, networking infrastructure, or deploying custom applications and software tools to meet production needs. A second area is information and data formats. This directly correlates to integration and interoperability challenges that cross all functions and remain a major cause for productivity issues. A third area is data availability and integrity. This area is now receiving needed attention in efforts to develop common practices for verification and validation of manufacturing data, such as the new ASME Subcommittee on Verification and Validation (V&V) for Manufacturing [16].

BARRIERS AND ENABLING TECHNOLOGIES

There are many significant barriers that can challenge manufacturers when addressing the requirements described previously. While some barriers can be easily addressed once properly understood, others may have conflicting goals that hinder effective resolution. However, recognizing these challenging barriers may be useful in creating new opportunities for appropriate standards and technology development.

Examples of significant barriers to achieve each decision-making function follow. Space does not permit us to be comprehensive, so instead we provide some example barriers that are often common for many manufacturers. We also describe potential solutions to these barriers where possible.

Function #1: Scope

Scoping requires that an organization's mission, objectives, stakeholders, and activities are understood and clearly identified, communicated, and prioritized. One of the greatest challenges in scoping is addressing the multiple viewpoints that are involved in an analysis. Often a superficial understanding that rests on semantic misunderstandings prevails. The misunderstanding may not be clear until much further in the decision-making process, which may create faulty assumptions and wasted efforts.

Scoping challenges often occur when trying to deploy strategic objectives as operational improvements [18]. While many may understand a strategic objective such as cutting costs, it can be difficult to see the larger perspective where cost cutting in one area may increase costs in other areas or in the future. Identifying the operational areas to target for improvement is part of the scoping challenge. A number of technologies and standards for documenting processes can be employed to gain a clear understanding of the systems, software, and people involved in an analysis. However, the practice of using these technologies may be inconsistent. Good measures of the impact of different processes on the larger system can also help in scoping an analysis problem, but obtaining such measures can be difficult.

Conflicting goals are often created because of scoping challenges. As an example specific to manufacturing operations, consider a company embarking on an energy savings undertaking. Looking at energy use and energy saving potentials in isolation would very likely affect overall productivity. Whereas looking at productivity in isolation may overlook energy saving potentials. An instance of this phenomenon is seen in strategies being developed to control machine downtime so as to maximize productivity and minimize energy use to the extent possible.

Function #2: Identify

Identification barriers can arise from a number of issues most important of which is perhaps the complexity of manufacturing operations. Asset management, a key activity, is crucial to being able to identify appropriate systems and information for an analysis. For example, an analysis focused on discovering a particular type of environmental impact or a security vulnerability will be dependent on identifying the equipment that could potentially be involved. Asset management should address changes to any system in a timely manner to enable the identification of the resources needed for an analysis. Often asset management has been a very manual process. New technologies are allowing for more automated and accurate asset management. However, many cultural, procedural, and technical barriers can exist when deploying these technologies.

Many analyses require detailed information on the flows of material, energy, and information within the manufacturing enterprise, as well as the capabilities of various assets in terms of manufacturing performance and sensing and data reporting. This information is necessary for planning detailed analysis. For example, to understand energy consumption in a manufacturing facility, it can be useful to know what systems already monitor energy use and the level of detail at which this monitoring occurs to determine the need for additional sensors.

Another challenge is understanding the amount of data needed to support analysis. For example, the frequency of data collection from a sensor and the reliability of the sensor data can depend on several downstream considerations, such as the effectiveness of analytics, the impact of data transmission on network bandwidth, the amount of available data storage, and the affordability of solutions. In addition, as more data is collected, the means by which data is presented becomes another barrier to its utility.

Decreased costs, increased adoption of recognized standards, and improved technology can be helpful in addressing these barriers. For example, standards, such as ISO 22400 [19] for manufacturing operations management, can help identify data that needs to be collected for analysis.

Function #3: Collect

Connecting devices, applications, and machines to the network, making the devices and their information recognized and accessible to approved users, and protecting the devices from unauthorized access are some of the challenges manufacturers face. Data collection can be impeded or prevented entirely by a variety of barriers. For example, a machine tool can often be a “black box” that accepts commands but rarely provides rich data in response. It can be difficult for operators to know when actual process parameters (e.g., cutting speed, feed) meet the nominal process parameters requested. Other data may be "hidden" by the controller and inaccessible even to trained practitioners. Sometimes manufacturers can add sensors to capture this information, but it can be difficult to integrate these sensors without interfering with the operation of the machine and potentially voiding warrantees. Even if certain components are physically accessible, there may be no practical interface to provide access to data. Sometimes a vendor may intentionally hide information or limit export capability to lock customers into a proprietary tool [20]. Vendors can also be forced to develop solutions that are intentionally different to avoid infringing on patents. Since patents and patent overlap can be very complex, dangers of patent infringement are a particularly challenging barrier [21] and can apply to other functional areas as well.

Function #4: Transmit

While some data transmission is straightforward, much of it is difficult and will remain so for a variety of reasons. As an example, security requirements and practices stand as a barrier to transmission. Current security practices include isolating machines from a network if the machines present a significant risk to being accessed inappropriately. This is often the case for machine tools, many of which use outdated operating systems that are no longer supported by vendors. Even when machines are on a network, other barriers may be present, such as requiring protection by manual interaction for access (e.g., multifactor authentication) that intentionally cannot be automated.

Other barriers to transmission relate to the physical environment in a manufacturing facility. For instance, wireless signals do not always operate as efficiently as designed due to interference from the shop floor. Furthermore, as manufacturing becomes more reliant on timely access to data, infrastructure maintenance takes on greater importance.

Function #5: Analyze

Analysis faces many barriers including availability of the appropriate data and the ease of use of analysis applications. Changing analysis algorithms may require data that was previously thought to be valueless and discarded [22]. Some analysis can be used in real time while others require more processing time than is available in real time. While the later are still valuable, understanding how to integrate them into a system is still challenging. Some algorithms may be proprietary and patented, which can restrict use or make them too expensive. Some algorithms are based on heuristics without guarantees of performance, runtime, or space consumption limiting the applicability. Finally, some black-box-type algorithms (such as neural networks) provide no easy way to assess their performance, which can make their use unreliable. For more advanced analysis techniques, such as machine learning, reliable educational material on when and how to use them during operations is often lacking.

Function #6: Share

Barriers related to sharing range from policy to technology. On the policy side, deciding what can be shared and with whom is challenging. Too much sharing can create the risk of revealing trade secrets, while too little sharing may cause an organization to deal with duplication of efforts, people working at cross purposes, and missed opportunities. Another challenge is deciding what data, information, and metrics are most likely to be of benefit to the recipient since extra information may result in wasted processing effort. On the technology side having a common strategy for sharing results is important. Many solution providers are now offering cloud-based platforms for facilitating sharing but these do not necessarily address the complex archiving needs of an enterprise whose business depends on detailed engineering capabilities [23],[24]. Furthermore, tracability of products back to the specific processes used in their production is growing more important.

Another important barrier is understanding what partners within the supply chain can be trusted with what data. Partners may have other data or relationships that can use data in a way that is not expected. For example, access to inventory levels intended to give supply partners better preparation for ramping up manufacturing can be used by those same suppliers to negotiate more competitively. Some data can be sanitized, but figuring out what or how much sanitization is necessary can be time consuming and must be potentially revisited before each sharing event.

Function #7: Retrieve

Barriers to retrival limit the ability to find the right information at the right time. Challenges exist in addressing context-based methods for searching and managing the traceability of data. There are few methods to organize content in ways that are intuitive to practitioners, and few common practices for maintaining data provenance. For example, when data information resides in a variety of formats, some being proprietary, it can be difficult to bring them into a common analytic framework for further analysis. Difficulties arise in connecting data from different sources in terms of semantics as well as temporally. In addition, tracing the lineage of the data used in an analysis is important for authoritative purposes as well as understanding potential sources of error. Long-term archiving of data may be appropriate so that analysis can be repeated in the future. In addition, any translation of data is likely to result in some loss of content. For example, when creating visualizations for human consumption, details of the analysis are often not directly available.

Examples of Solutions to Overcome Barriers

Three types of solutions that address most barriers are standards, reference data, and technology. For example, dealing with multiple formats or multiple interfaces can be addressed with a standard. Similarly, technology advancements can provide solutions to some barriers. For example, improved modeling tools and methods allow for more effective and efficient simulations. Lastly, reference data can be helpful to implementors by saving them from the effort of exploring these ideas anew.

Admittedly, all of these approaches are limited to the degree by which they can surmount barriers and sometimes they can present new barriers themselves. While standards can be helpful, their development often takes considerable time and effort, and there is always the risk that the standard may not be adopted. Numerous organizations have evolved with different approaches to standards building as a result [5]. Still standards can themselves become a barrier. For example, there is no point to seek standardization for a technology that will have a relatively limited lifespan, especially when the time needed for a standard development effort exceeds the life of the technology. Indeed, premature standards can inadvertently lock users into inferior solutions.

An alternative to standards are "best practices," where a group of companies or an industry sector agrees to a common set of implementation guidelines for a standard. Because the agreed-to best practices are not part of the "official" standard, they can be more easily modified in response to technological change or business drivers. An example of a best-practices effort in support of manufacturing is the CAx Implementor Forum, which is a group of Computer Aided Design software vendors, users, and solution providers who publish guidance for implementing ISO 10303-242. ISO 10303-242 is a standard for the representation and exchange of digital 3D design data with annotations that provides product and manufacturing information needed for fabrication 25,26. Another best-practices example is the MTConnect C++ Agent, which has been provided to enable implementation of the communications protocols of the standard [27].

Similarly, technology can also offer further challenges as well as solutions. When solutions work, they may come with trade-offs and often sacrifice flexibility due to a lack of interoperability between competing vendor solutions.

Wireless technology is an example of several of these issues. Wireless was a technological advance over wired connections that allowed mobile solutions as well as easier placement of sensors and controllers. Very quickly after its introduction, standards were offered to address incompatibility issues and proprietary lock-in. However, there are currently many incompatible wireless standards including some with proprietary implementations, such as IEEE 802.15.1 (Bluetooth Classic), Bluetooth Low Energy, IEEE 802.11 (WLAN), and IEEE 802.15.4 (ZigBee, WirelessHART, ISA 100) [28].

SUMMARY

The successful deployment and use of data-driven decision-making and other smart manufacturing technologies will depend on educating manufacturers and technology developers about the best ways to leverage the value of these solutions. Manufacturers need support to navigate the breadth of solutions in the market, and technology developers must understand the most compelling use cases to ensure that their solutions meet the needs of industry. The first step towards assuring the performance of smart manufacturing technologies is to develop a means for the manufacturing community to pool its knowledge and collaborate to identify problems and collect solutions and best practices. Helu et al. [10] proposed a collective knowledgebase to provide a means of achieving this goal. We have extended the idea in this paper by describing a framework to organize the content of the knowledgebase and by identifying some common activities for and barriers to data-driven decision making in manufacturing.

While the proposed framework has focused on data-driven decision making, it may be used for other aspects of smart manufacturing technology, such as increased specialization to accommodate advanced materials, increased use of model-based engineering [29],[30], and increased deployment of collaborative robotic systems. Future work will focus on expanding the content in the framework as well as providing more depth to the initial content generated for this research. We hope to engage the larger manufacturing community in this effort to ensure its comprehensiveness and accuracy. Bringing together experts, though, requires an effective operational model for the knowledgebase, which is another goal of future work. If successful, we believe that the knowledgebase can spur innovation by identifying high impact areas for standards and technologies that help deliver on the promise of smart manufacturing and ensure the success of manufacturing.

ACKNOWLEDGMENTS AND DISCLAIMER

The authors would like to acknowledge Kiwook Jung and Swee Leong for their support in completing this research. Certain commercial systems are identified in this paper. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology. Nor does it imply that the products identified are necessarily the best available for the purpose.

REFERENCES

[1] Davidson, M. and Goodwin, G., 2014, "2013-2014 Manufacturing Metrics that Really Matter Summary Report," LNS Research, http://www.lnsresearch.com/research-library/research-articles/2013-2014-manufacturing-metrics-that-really-matter-summary-report, accessed 05/12/2016.

[2] Hopkins, M. S., Kruschwitz, N., Haanaes, K., Kong, M. T., Arthur, D., and Reeves, M., 2011, "New Sustainability Study: The 'Embracers' Seize Advantage," MIT Sloan Management Review, Spring 2011.

[3] AMP2.0 Steering Committee, 2014, "Report to the President: Accelerating U.S. Advanced Manufacturing," https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/amp20_report_final.pdf, accessed 05/12/2016.

[4] Lu, Y., Morris, K., and Frechette, S., 2015, "Standards Landscape and Directions for Smart Manufacturing Systems," 2015 IEEE International Conference on Automation Science and Engineering (CASE), Gothenburg, Sweden, pp. 998-1005.

[5] Lu, Y., Morris, K., and Frechette, S., 2016, "Current Standards Landscape for Smart Manufacturing Systems," NIST Technical Note 8107, National Institute of Standards and Technology, Gaithersburg, MD.

[6] O'Marah, K. and Manenti, P., 2014, "The Internet of Things Will Make Manufacturing Smarter," Industry Week, http://www.industryweek.com/manufacturing-smarter, accessed 05/12/2015.

[7] Accenture, 2015, "CEO Briefing 2015: From Productivity to Outcomes: Using the Internet of Things to drive future business strategies," https://www.accenture.com/t20150527T211103__w__/fr-fr/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/fr-fr/PDF_5/Accenture-CEO-Briefing-2015-Productivity-Outcomes-Internet-Things.pdf, accessed 02/15/2016.

[8] Littlefield, M. and Goodwin, G., 2015, "The Industrial Internet of Things and Big Data Analytics: A Coming Manufacturing Revolution," LNS Research, http://www.lnsresearch.com/research-library/research-articles/the-industrial-internet-of-things-and-big-data-analytics-a-coming-manufacturing-revolution, accessed 05/12/2016.

[9] Waurzyniak, P., 2015 "Why Manufacturing Needs Real-Time Data Collection," Manufacturing Engineering, October 2015, pp. 53-61.

[10] Helu, M., Morris, K., Jung, K., Lyons, K., and Leong, S., 2015, "Identifying Performance Assurance Challenges for Smart Manufacturing," Manufacturing Letters, 6, pp. 1–4.

[11] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A., 2015, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82r2, National Institute of Standards and Technology, Gaithersburg, MD.

[12] MTConnect Institute, 2015, MTConnect v. 1.3.1, http://www.mtconnect.org/standard/, accessed 05/12/2016.

[13] Albert, M., 2012, "MT Connect: Two Shops Share Their Experience," Modern Machine Shop, August 2012, http://www.mmsonline.com/articles/mt-connect-two-shops-share-their-experience, accessed 05/12/2016.

[14] Helu, M. and Weiss, B., 2016, "The Current State of Sensing, Health Management, and Control for Small-to-Medium-Sized Manufacturers," Proceedings of the ASME 2016 International Manufacturing Science and Engineering Conference, Blacksburg, VA, to appear.

[15] MITRE Corporation, 2015, "Common Weakness Enumeration," https://cwe.mitre.org/, accessed 05/12/2016.

[16] ASME, 2016, "Committee Page: V&V 50 Verification and Validation of Computational Modeling for Advanced Manufacturing," https://cstools.asme.org/csconnect/CommitteePages.cfm?Committee=101978604, accessed 05/12/2015.

[17] National Institute of Standards and Technology, 2014, "Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0," http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, accessed 05/12/2016.

[18] Jung, K., Morris, K. C., Lyons, K. W., Leong, S., and Cho, H., 2015, "Mapping Strategic Goals and Operational Performance Metrics for Smart Manufacturing Systems," Procedia Computer Science, 44, pp. 184–193.

[19] ISO, 2014, "Automation systems and integration – Key performance indicators (KPIs) for manufacturing operations management – Part 2: Definitions and descriptions," ISO 22400-2:2014.

[20] Commission of the European Communities, 2004, "Commission Decision of 24.03.2004 relating to a proceeding under Article 82 of the EC Treaty," C(2004)900 final, Brussels, Belgium.

[21] Shapiro, C., "Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard Setting," Innovation Policy and the Economy, A. B. Jaffe et al., eds, MIT Press, Cambridge, MA, 1, pp. 119-150.

[22] Libes, D., Shin, S., and Woo, J., 2015, "Considerations and Recommendations for Data Availability for Data Analytics for Manufacturing," 2015 IEEE International Conference on Big Data (Big Data), Santa Clara, CA, pp. 68–75.

[23] Barbau, R., Lubell, J., Rachuri, S., and Foufou, S., 2014, "Towards a Reference Architecture for Archival Systems: Use Case With Product Data," ASME Journal of Computational Information Science in Engineering, 14(3), 031005 (Apr 28, 2014).

[24] ISO, 2012, "Space data and information transfer systems – Open archival information system (OAIS) – Reference model," ISO 14721:2012.

[25] PDES, Inc. and ProSTEP iViP, (n.d.), "CAx Implementor Forum," https://cax-if.org/index.html, accessed 05/06/2016.

[26] Lipman, R. and Lubell, J., 2015, "Conformance Checking of PMI Representation in CAD Model STEP Data Exchange Files," Computer-Aided Design, 66, pp. 14–23.

[27] MTConnect User's Portal, 2015, "MTConnect C++ Agent," http://mtcup.org/wiki/C%2B%2B_Agent, accessed 05/12/2016.

[28] Andersson, M., 2013, "Wireless Technologies for Industrial Applications, Version 2.2," connectBlue, http://www.connectblue.com/fileadmin/Connectblue/Web2006/Documents/White_papers/Industrial_Bluetooth.pdf, accessed 05/12/2016.

[29] Lubell, J., Chen, K., Horst, J., Frechette, S., Huang, P., 2012, "Model Based Enterprise/Technical Data Package Summit Report," NIST Technical Note 1753, Gaithersburg, MD.

[30] Hedberg Jr., T., Lubell, J., Fischer, L., Maggiano, L., Barnard Feeney, A., 2016, "Testing the Digital Thread in Support of Model-Based Manufacturing and Inspection," Journal of Computational and Information Science in Engineering, 16(2), 021001 (Mar 08, 2016).

Proceedings of the ASME 2016 International Manufacturing Science and Engineering Conference
MSEC2016
June 27-July 1, 2016, Blacksburg, Virginia, USA

MSEC2016-8783

THE CURRENT STATE OF SENSING, HEALTH MANAGEMENT, AND CONTROL FOR SMALL-TO-MEDIUM-SIZED MANUFACTURERS

Moneer Helu
National Institute of Standards and Technology
Gaithersburg, MD, USA

Brian Weiss
National Institute of Standards and Technology
Gaithersburg, MD, USA

KEYWORDS
Sensing, control, diagnosis, prognosis, SME

ABSTRACT

The development of digital technologies for manufacturing has been challenged by the difficulty of navigating the breadth of new technologies available to industry. This difficulty is compounded by technologies developed without a good understanding of the capabilities and limitations of the manufacturing environment, especially within small-to-medium enterprises (SMEs). This paper describes industrial case studies conducted to identify the needs, priorities, and constraints of manufacturing SMEs in the areas of performance measurement, condition monitoring, diagnosis, and prognosis. These case studies focused on contract and original equipment manufacturers with less than 500 employees from several industrial sectors. Solution and equipment providers and National Institute of Standards and Technology (NIST) Hollings Manufacturing Extension Partnership (MEP) centers were also included. Each case study involved discussions with key shop-floor personnel as well as site visits with some participants. The case studies highlight SME's strong need for access to appropriate data to better understand and plan manufacturing operations. They also help define industrially-relevant use cases in several areas of manufacturing operations, including scheduling support, maintenance planning, resource budgeting, and workforce augmentation.

INTRODUCTION

The role of sensing, monitoring, and control in any system is to observe data, use the collected data to determine the system's state, and apply the generated knowledge to optimize and/or improve the system's performance. To better meet these goals, the development of sensing, monitoring, and control for manufacturing systems has progressed from human oversight to more sophisticated sensor-based monitoring systems [1]. In-process, sensor-based monitoring systems are considered an essential means to meet increasingly tightening requirements on the precision, quality, and performance of manufacturing processes [2-3]. In addition, the growth and accessibility of digital (i.e., information and computer-based) technologies for manufacturing has provided industry with new opportunities to collect and use data to improve the control of engineering and production systems [4-5]. These technologies have the potential to improve the competitiveness of manufacturing by reducing cost, improving productivity, ensuring first-pass success, and augmenting existing capabilities in the workforce.

Smart manufacturing, digital manufacturing, cloud manufacturing, cyber-physical systems, the Industrial Internet of Things (IIoT), and Industry 4.0 are some of the terms that have been used to describe the increasing use of digital technologies in manufacturing and industry in general. Despite the various terms that exist in the literature, these areas of research and development have several common themes. First, all describe some form of interoperability between systems across the product lifecycle (from design to end of life) and the manufacturing enterprise (from the shop floor through the supply chain) [4-6]. Second, this interoperability enables the generation of actionable intelligence through the efficient and effective use of collected data and information. Finally, the generated intelligence supports decision making through improved monitoring, analytics, modeling, and simulation.

One area of manufacturing that has benefited from digital technologies is prognostics and health management (PHM). A recent industry survey found that maintenance and machine performance are two of the most important benefits of the Industrial Internet of Things [7]. While PHM is typically considered in the context of process, equipment, or system health and maintenance, it is a broader field that encompasses performance measurement, condition monitoring, diagnosis, and prognosis [8-9]. The goal of PHM in manufacturing is to apply robust sensing, monitoring, and control to best respond to planned and unplanned changes in the performance of manufacturing systems [9]. Meeting this goal requires sensing and control strategies integrated across the manufacturing

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. SP-326
Approved for public release. Distribution is unlimited.

Downloaded From: http://proceedings.asmedigitalcollection.asme.org/ on 09/27/2016 Terms of Use: http://www.asme.org/about-asme/terms-of-use

enterprise that can generate and respond to high-quality intelligence on the current performance of production systems.

There are a number of digital technologies and standards that have been introduced that support one or more requirements of PHM. Liang et al. [3], Gao et al. [10], and Teti et al. [11] provide a thorough summary of much of the research and development of these solutions and highlight relevant examples in the market. The market contains software solutions that support manufacturing operations management by monitoring shop-floor data and providing dashboards that display metrics and key performance indicators (KPIs). Some of these solutions also include platforms that provide additional intelligence based on the collected shop-floor data, such as classifying productive and nonproductive periods for equipment. Examples of these software include System Insights VIMANA, TechSolve ShopViz, FORCAM Force, and Memex MERLIN [12-13]. In addition, some manufacturers have designed their own software solutions, such as ITAMCO's QUPID system, which is a mobile application that captures and provides operational information to shop-floor personnel [12]. Each of these solutions leverages the MTConnect standard, which is an open-source standard that enables interoperability between shop-floor devices, equipment, and applications [14].

Even though digital technologies are increasingly available and accessible to manufacturers, they are not yet extensively used in industry. For example, some experts have estimated that only 5 % of machines in manufacturing facilities are currently being monitored digitally [13]. Part of the problem is that manufacturers have found it increasingly challenging to navigate the breadth of new technologies available to industry [5]. This difficulty is further compounded by technologies developed without a good understanding of the capabilities and limitations of the manufacturing environment. This is especially true for small-to-medium enterprises (SMEs), which have typically been an underserved market segment. The goal of the research presented in this paper is to enable the development of PHM solutions appropriate for industry by describing industrially-relevant use cases. To describe these use cases, we first study existing manufacturing operations through a series of case studies to identify the relevant needs, priorities, and constraints of industry. Our focus in these case studies is on performance measurement, condition monitoring, diagnosis, and prognosis.

CASE STUDY APPROACH

We designed the case studies presented in this paper to target three research areas. First, we wanted to describe the equipment, infrastructure, and configuration of manufacturing systems common in industry. Second, we wanted to identify the common metrics and best practices used by industry in their sensing, health management, and control activities. Finally, we wanted to define the common problems, failures, and bottlenecks for manufacturing processes, equipment, and systems. These case studies distinguished between large and SME manufacturers so that we could better capture the often substantially different considerations specific to each environment. We have presented the results of case studies conducted with SME manufacturers in this paper. SME manufacturers were defined as those organizations with less than 500 employees [15]. Jin et al. [16] have presented more information about the case studies conducted with large manufacturers.

Case-study participants were primarily discrete manufacturers that used subtractive processes and operated within a variety of industrial sectors, including aerospace, automotive, chemical, energy, mining, personal care, petroleum, pharmaceutical, and shipping. The participants were grouped into three classifications based on workforce size and role within the supply chain: small contract manufacturer, medium contract manufacturer, and original equipment manufacturer (OEM). Contract manufacturers (sometimes referred to as "job shops") are outsourcing organizations that contract with other companies to produce parts owned by the customer. OEMs are organizations that produce parts owned internally or by a parent company. In addition to SME manufacturers, the case-study effort also included solution and equipment providers and National Institute of Standards and Technology (NIST) Hollings Manufacturing Extension Partnership (MEP) centers that work with the SME manufacturing community.

Interactions with prospective case-study organizations typically began with an introductory telephone call to present the objectives of the effort and discuss any potential concerns. We followed this initial interaction with more detailed discussions with key shop-floor personnel (for manufacturers) or appropriate engineering personnel (for solution and equipment providers and NIST MEP centers) that focused on:

- Metrics and key performance indicators (KPIs)
- Maintenance activities and strategies
- Best operational practices and examples of successful improvement efforts
- Methods used to monitor, respond to, and improve interactions with suppliers

The goal of these conversations was to identify the common approaches used by the organization being studied as well as the critical drivers and limitations that motivated these approaches. The discussions did not include any predetermined questions and were allowed to evolve as the participant preferred to better understand the greatest concerns for SME manufacturers even if those concerns fell outside of the scope of this study. Site visits and detailed facility tours were conducted for a subset of participants based on availability. These visits focused on further demonstration and explanation of specific systems, issues, and challenges highlighted previously during the discussions. We followed up with participants as needed to clarify previous discussions.

Downloaded From: http://proceedings.asmedigitalcollection.asme.org/ on 09/27/2016 Terms of Use: http://www.asme.org/about-asme/terms-of-use

Table 1. Description of three generic SMEs that reflect the SMEs considered by the case studies.

	Contract Manufacturer		**Original Equipment Manufacturer (OEM)**
	Small	**Medium**	
# of Employees	25 total (25 on shop floor)	150 total (100 on shop floor)	100 (75 on shop floor)
Sales Revenue	$5 million	$20 million	$50 million
Industry Sectors	Automotive, Food, Personal Care, Pharmaceutical	Aerospace, Chemical, Energy, Mining	Chemical, Petroleum, Pharmaceutical, Shipping
# of Part Numbers Managed	5000 (≈50 % under active contract)	5000 (≈20 % under active contract)	100000+

CASE STUDY FINDINGS

We present the findings from the case studies by describing a generic SME within each classification group. Table 1 provides an overview of each of the three generic SMEs. The findings for each generic SME has been developed by aggregating the data generated from the case studies. We select this approach to highlight the overall themes we encountered instead of issues specific to one organization.

Small Contract Manufacturer

Table 2 provides a summary of the findings for the Small Contract Manufacturer (referred to as "SCM"). The SCM has the smallest workforce and lowest sales revenue of the three generic SMEs. It also usually earns the smallest margin per part given the need to remain cost competitive in the market. The SCM's small workforce is employed fully on the shop floor and typically in multiple roles. This flexibility leans the workforce and addresses a significant challenge the SCM shares with all SME manufacturers: finding good operators and machinists. This challenge is especially problematic for the SCM since it needs a relatively diverse set of skills given the variety of contracts it may win, but it often lacks the resources to train and retain talent. In fact, the SCM knows that larger manufacturers poach its talent to avoid having to invest in finding and training employees. This is a significant disincentive for the SCM to invest its limited resources in advanced manufacturing technologies.

The need for flexibility is paramount for the SCM when considering equipment needs. Table 1 highlights the relatively diverse set of industry sectors served by the SCM. It also shows the relatively large number of distinct part numbers that the SCM must manage, which is driven by the need to bid on a large variety of contracts to ensure a steady flow of business. The SCM has more machines (35) than employees to provide as wide a range of manufacturing process capabilities as feasible, such as milling, turning, grinding, electric-discharge machining, stamping, and forming. These machines are also of varied age and equipment make since the SCM purchases equipment with the best value relative to capabilities regardless of the vendor. The SCM also has inspection capabilities primarily in the form of hand tools, such as calipers and gauges. It would like to procure a coordinate measuring machine (CMM) eventually to allow it to bid on more lucrative contracts, such as those in aerospace, which require certification and traceability. Each employee is assigned to two-to-three machines to ensure that somebody is always available to run any machine as needed.

The SCM uses some software resources to support its operations. Cost and a lack of in-house expertise are generally the two largest considerations when the SCM invests in software resources, and so these resources tend to be standard packages with relatively limited capabilities and features. Solidworks is the computer-aided design (CAD) package used in the SCM, and part programming is often completed manually. For those machinists willing to use computer-aided manufacturing (CAM) packages for programming, there is a strong preference for MasterCam, but the SCM does not currently have licenses for all of its staff. The SCM also uses DBA Manufacturing to support manufacturing resource planning (MRP), but there is interest in switching to E2 instead since the SCM believes that E2 better fits its needs. In either case, the SCM relies on manual entry of data to keep its systems simple to use and maintain.

Table 2. Summary of generic Small Contract Manufacturer.

Operational Characteristics	• Emphasis on flexibility and broad skill set in workforce • Diverse equipment of varied age and capability • Limited resources that favor simple solutions
Metrics and Key Performance Indicators	• Gross margin • Basic utilization • On-time delivery
Maintenance Approach	• Primarily reactive • Limited preventative
Supply Chain Interactions	• No tracking or monitoring
Primary Business Challenges	• Workforce development • Equipment availability
Primary Technology Interests	• Dashboards that quantify performance • Detailed operational information • Estimation support
Primary Technology Concerns	• Potential disruption to operations • Lack of in-house expertise to deploy and maintain solutions

Downloaded From: http://proceedings.asmedigitalcollection.asme.org/ on 09/27/2016 Terms of Use: http://www.asme.org/about-asme/terms-of-use

Gross margin is the most important metric that the SCM tracks even though flexibility tends to be its most important asset. Gross margin is profit as a percentage of revenue. Basic utilization (i.e., the ratio of the time that equipment is in cycle to total time) is also important, but the SCM often runs at ≈70 % utilization at best since some machines may not be needed for the current set of work. Both metrics reflect the SCM's ability to maximize its efficiency when faced with limited resources and the need to deliver a large variety of parts. On-time delivery is another important metric that the SCM uses to understand customer satisfaction since speed tends to be an important part of a winning contract and successful customer interaction that leads to future business.

Despite its emphasis on gross margin and equipment utilization, maintenance is not an area where the SCM invests heavily. The labor challenges faced by the SCM prevents it from developing a dedicated maintenance staff. Instead, the SCM relies primarily on a reactive maintenance strategy that is bolstered by some preventative maintenance based on the equipment vendor's guidelines. The staff are often unable to recognize deficiencies in performance or other characteristics that indicate an increased risk of failure, which leads to a relatively high occurrence of downtime events. Every downtime event requires external support since the SCM's staff lack the training to respond to and resolve many maintenance issues that occur.

The increasingly competitive marketplace for the SCM has forced it to reconsider many of its operational strategies in order to boost its gross margin and equipment utilization. To do so, the SCM must overcome its two primary business challenges: workforce development and equipment availability. The SCM believes that technological advances in sensing, health management, and control can augment and improve the capabilities of its staff. While many of the SCM's technology interests are relatively "low-hanging fruit," such as dashboards that quantify employee performance and encourage improvements, other interests fall within active areas of research in digital manufacturing. For example, the SCM wants to use data and information from all of its systems to quantify the operational status of its equipment and provide intelligence that explains why its equipment may not be running at peak performance. Such knowledge can improve its preventative maintenance capabilities by identifying machines that require attention as well as support capital investment decisions to replace machines nearing the end of useful life. It can also support estimation activities by examining how well the SCM meets its production targets, which can improve the SCM's ability to bid appropriately for new contracts.

New opportunities presented by digital and PHM technologies have encouraged the SCM to explore ways to address its varied business interests. It has begun to network six of its 35 machines in a project with a solution provider who has provided a dashboard that presents basic operational information, such as machine cycle and basic utilization. As the SCM expands these capabilities, its biggest concern is any disruption to its operations as its machines and systems are upgraded to accommodate this new technology. This is an especially large concern for the SCM since it must rely on external support to deploy and maintain these technologies. Interestingly, cybersecurity is not a large concern for the SCM because it does not deal with overly sensitive information (e.g., export-control work). However, this could also be due to a lack of experience with cybersecurity.

Medium Contract Manufacturer

Table 3 provides a summary of the findings for the Medium Contract Manufacturer (referred to as "MCM"). Unlike the SCM, the MCM provides more specialized services (in terms of manufacturing process capabilities provided to customers) and tends to have a more focused strategy when bidding for contracts. The MCM in this example focuses on machining metal components that require relatively large work volumes in excess of 64 m^3. Even though the MCM serves different industry sectors and manages a relatively large number of part numbers (as shown in Table 1), the types of parts that the MCM produces are typically very similar because of the MCM's specialized capabilities. These capabilities and its larger workforce size provide the MCM with a higher sales revenue than the SCM, however the margin per part can be small, especially if the MCM does not bid appropriately for a contract. In general, though, the market pressures tend to be

Table 3. Summary of generic Medium Contract Manufacturer.

Operational Characteristics	• Specialized manufacturing process capabilities • Standardized equipment and systems • Engineering, maintenance, and administrative support
Metrics and Key Performance Indicators	• Basic utilization • Start time versus in-cycle time • Rework cost per direct labor hour • Part-program conformance
Maintenance Approach	• Primarily reactive • Limited preventative
Supply Chain Interactions	• No tracking or monitoring
Primary Business Challenges	• Equipment availability • Process planning and scheduling • Workforce culture
Primary Technology Interests	• Condition-based maintenance • Near-real-time supervisory monitoring and control of shop-floor operations • Estimation and scheduling support
Primary Technology Concerns	• Lack of common data interfaces and protocols • Cybersecurity requirements • Low data volumes for analysis

Downloaded From: http://proceedings.asmedigitalcollection.asme.org/ on 09/27/2016 Terms of Use: http://www.asme.org/about-asme/terms-of-use

lower on the MCM than the SCM since far fewer organizations can provide comparable services to customers.

The MCM's specialization allows it to also focus on more targeted training for its workforce and less varied processes and equipment. The MCM has dedicated engineering, maintenance, and administrative staff in addition to its operators and machinists on the shop floor. All of its fabrication equipment are either three- or five-axis machining centers with large work volumes. This equipment is made by one of three vendors who specialize in this type of equipment, and all of the equipment uses the same type of controller. The MCM is a big proponent of standardization to avoid any issues that can arise with heterogeneous systems and interfaces and to enable its staff to work with multiple machines. However, standardization of this sort also creates unique problems for the MCM. First, the MCM is locked into a limited choice of equipment, which can significantly raise the cost of capital investments. Second, the MCM must seek specific skills in its workforce, which can complicate the already difficult process of hiring talent for all SMEs. Finally, the size and specialization of its equipment forces a high burn rate (or cost to run the equipment in excess of income) when the machines experience downtime: $225/hr on average. This high burn rate drives many of the operational decisions of the MCM as well as its strong interest in health management.

Another significant difference between the SCM and MCM is the MCM's ability to devote resources towards software to support its operations. Here again there is a strong preference for standardization in the choice of software. Solidworks and MasterCAM are the CAD and CAM packages of choice, respectively. The MCM also uses E2 to support MRP, but it is interested in exploring other software options since it would prefer a more customizable MRP option. The MCM also has a strong interest in investing in other productivity resources, such as the various MTConnect-enabled solutions discussed in the Introduction. Because of its standardized systems, these types of productivity solutions become much simpler to deploy within the MCM's facility. However, the MCM still has to contend with the challenges posed by manual data entry when using any productivity solution.

The MCM tends to focus its monitoring efforts on more detailed metrics and KPIs that influence gross margin. The two most important metrics are basic utilization and start time versus in-cycle time (i.e., the percentage of cycle time that the machine is in process as opposed to setup). Two other metrics that the MCM has started to track are rework cost per direct labor hour and part-program conformance (i.e., the percentage of time that a part program is not modified by the operator or machinist). The interest in all four metrics is tied to the high burn rate of the MCM's equipment. Given the relatively high cost to run its equipment, the MCM wants its equipment to produce chips with minimal delays due to setup, maintenance, failure, rework, or needed modifications to part programs.

The MCM lacks a sophisticated maintenance program despite its interest in health management and its dedicated maintenance staff. It relies primarily on reactive maintenance and a "band-aid" approach because of the extremely high costs associated with unplanned downtime. These costs have incentivized preventative maintenance in the past, but the MCM's staff never fully embraced these strategies because of a belief in their high cost. Currently, though, maintenance has grown to become the biggest cost for the MCM as it has experienced unexpected failures every few days that usually last one or more days. These failures are almost always due to a traditional machine fault (e.g., bearing failure) and can be expensive to resolve given the specialized nature of the equipment. Machine calibration has also started to become a significant issue as the MCM's equipment ages. For these reasons, the MCM is reintroducing preventative maintenance, training its operators and machinists to observe events that indicate machine faults and failures, and starting to collect and track maintenance data for its machines. The MCM has also started to explore options for condition-based maintenance and scheduling support to minimize the frequency and impact of unexpected downtime events.

The MCM also faces other significant planning and labor issues that it hopes can be resolved using improved sensing, health management, and control. For example, the MCM relies on tribal knowledge for estimation, which has resulted historically in underestimates that can be up to 200 % below the actual cost. Part of this challenge can be traced back to maintenance problems, but the MCM also believes that it may be due primarily to modifications that machinists make to part programs (which can be caused by poor programming or inexperience in machining) as well as general cultural issues within its workforce. The MCM does not yet have the data needed to understand its estimation issues fully, but they would like to provide their engineering and shop-floor staff more information from near-real-time supervisory monitoring and control systems for shop-floor operations. Specifically, they are interested in productivity solutions that build upon existing technologies, which capture basic utilization and cost, and add detailed information to explain why equipment may not be productive. They are also interested in dynamic scheduling resources that allow them to respond to operational changes. The MCM believes that both solutions can support their efforts to address their cultural problems and keep their workforce engaged. For example, the MCM's engineering and management staff has observed that productivity decreases when the shop-floor staff believe that there is less work in the queue. By having the ability to reliably schedule work beyond two weeks of operations, the MCM hopes to incentivize higher productivity from its staff. Previous efforts focused on rework highlight the potential of these solutions for the MCM: rework was reduced by 50 % when the MCM tracked rework and highlighted poor performance.

Existing improvement efforts emphasize the biggest concerns that the MCM faces when deploying digital manufacturing and PHM technologies. Many of these concerns are due to the obstacles created by networking systems that lack common data interfaces and protocols. Even though it standardized much of its equipment, the MCM's equipment and

Downloaded From: http://proceedings.asmedigitalcollection.asme.org/ on 09/27/2016 Terms of Use: http://www.asme.org/about-asme/terms-of-use

software resources do not connect well with each other. Internal cybersecurity requirements further complicate data interoperability. Interoperability issues also extend to licensing: vendors who provide product-lifecycle management (PLM) and/or enterprise-resource planning (ERP) solutions have not been receptive to supporting the MCM's efforts to network its existing systems. Instead, these vendors demand that the MCM invest in new software packages that the MCM lacks financial and technical resources to deploy. Even if it resolves all of these issues, the MCM often lacks sufficient data to support analysis because of the relatively low volumes of unique parts that it produces. This is a common problem for all contract manufacturers and underscores the need for appropriate verification and validation tools for digital and PHM technologies and solutions.

Original Equipment Manufacturer

Table 4 provides a summary of the findings for the Original Equipment Manufacturer (referred to as "OEM"). The OEM has the highest sales revenue of the three generic SMEs presented in this paper, but it has a relatively lean workforce (see Table 1). It can have a smaller workforce than the MCM because it is more specialized than the MCM. Instead of delivering parts based on types of manufacturing capabilities, the OEM produces all of the components for five product lines. This is why the OEM manages a large number of part numbers: each component has its own set of part numbers, but overall product variation is minimal and created only because of differences in size and material. Product variation is even smaller in other OEMs that produce only one component of various sizes for a parent organization. The volume for each part number is low in both situations since the OEM typically produces parts to order.

Similar to the MCM, the OEM's specialization allows it to invest in machining centers from one of three vendors. The OEM prefers standardization across all of its equipment, but it has shifted from one vendor to another over time to balance costs relative to capabilities. All of the OEM's equipment use the same type of controller to allow its staff to work with any machine. The OEM's specialization and resources also allow it to organize its equipment into a number of cells with targeted automation so that it needs fewer operators and machinists. One negative consideration for the OEM is that its equipment can be very expensive to operate and maintain. For example, the OEM has purchased an entire inventory of spare parts that it stores in a separate warehouse because of the difficulty in securing needed parts quickly. It is for these reasons that the OEM is extremely interested in developing additional maintenance and health management capabilities.

Because it has more resources than the two contract manufacturers, the OEM can provide additional operational support to its shop-floor personnel. It employs dedicated engineering, maintenance, and administrative staff, and it purchases more sophisticated software packages when needed. For example, the OEM uses SAP for ERP support and has invested in a few of the MTConnect-enabled tools described in the Introduction. Its CAD and CAM packages are Solidworks and MasterCAM, respectively, since this is the preference of its engineering and shop-floor staff. The OEM has also invested in a tooling management system so that it can track and optimize its tooling costs, which are another large expenditure.

The primary metrics that the OEM tracks are basic utilization and process efficiency, which is a measure of the setup and run time for a job relative to a standard part. Both choices are motivated by the relatively high cost to run its equipment. The OEM also tracks its customer satisfaction by monitoring delivery and lead times and conformance to estimation (i.e., ratio of actual to estimated cycle time for each process step). All of these measurements are complicated by the large work in progress (WIP) that the OEM must manage: it usually has 400 to 600 orders in its facility as WIP because it is the sole producer of its products. Also, the OEM currently relies on manual input of data, which delays its information by one day, but it is currently working to network all of its systems to automate data collection. The OEM hopes to automate data collection across its supply chain to improve existing processes that support the traceability requirements on its products. However, it would like to ensure that data shared across the supply chain is strictly controlled to protect sensitive information and intellectual property.

Table 4. Summary of generic Original Equipment Manufacturer.

Operational Characteristics	• Very specialized: produces five lines of the same product • Standardized systems based on cost and capability • Engineering, maintenance, and administrative support
Metrics and Key Performance Indicators	• Basic utilization • Process efficiency • Delivery and lead times • Conformance to estimation
Maintenance Approach	• Primarily preventative • Strong interest in predictive
Supply Chain Interactions	• Minimal based on traceability requirements
Primary Business Challenges	• Equipment availability • Scheduling • Foreign competition • Workforce development
Primary Technology Interests	• Predictive maintenance • Automation • Dynamic scheduling • Near-real-time supervisory monitoring and control
Primary Technology Concerns	• Lack of common data interfaces and protocols • Cybersecurity requirements • Low data volumes for analysis

Downloaded From: http://proceedings.asmedigitalcollection.asme.org/ on 09/27/2016 Terms of Use: http://www.asme.org/about-asme/terms-of-use

One role of the OEM's primary metrics and KPIs is to manage the maintenance and health of its equipment. The OEM relies on preventative maintenance broken down into daily, weekly, and monthly activities managed by its maintenance staff. Larger overhauls of its equipment occur every few years based on the vendor's specification and with the vendor's assistance. As we have mentioned previously, the OEM would like to invest in predictive maintenance capabilities. It has conducted several equipment studies to understand common failure modes, but these studies have yet to yield enough data to support operational decision making. It has also trained its operators and machinists to provide anecdotal data about the state of its equipment. The OEM is ready to invest in solutions to collect more maintenance data, but it would like support to decide what data to collect and how to collect it so that operations are minimally disrupted. Like all SMEs and manufacturers in general, the OEM would like to avoid "big data" since it does not have the expertise or resources to manage it. Ultimately, the OEM shares the MCM's hopes that advances in digital manufacturing and PHM technologies yield near-real-time supervisory monitoring and control systems that can explain why equipment is or is not running productively.

The OEM also faces other significant challenges in addition to maintenance. Increasing competition from foreign companies making similar products has forced the OEM to focus on ways to reduce changeovers and increase equipment utilization to cut costs. These demands are made more difficult by the fact that the OEM makes products to order, which creates small batch sizes (typically less than 10). These factors have further motivated the OEM to collect data from its production systems. It would like to use this data to generate dynamic scheduling capabilities that allow it to respond quickly and effectively to changes in the performance of its systems (e.g., due to unexpected downtime) as well as the market or supply chain. They also want to use this data to address existing labor challenges. Like the contract manufacturers, the OEM finds it difficult and expensive to hire and train talent. They often lose trained operators and machinists to large manufacturers because they cannot compete on wages. The OEM hopes that advances in digital manufacturing and PHM technologies can promote automation in ways that simplify operations for and augment the skills of its staff. One extension of these capabilities that the OEM has started to explore is the application of data interoperability across the product lifecycle (also referred to as the "digital thread") to understand the accuracy of their expectations about their operations. For example, the OEM would like to know if decreases in product quality are due to errors in design, planning, or manufacturing; the typical assumption is that quality issues are created by manufacturing, but this can hide other opportunities to improve the overall product design and manufacturing process.

Despite the promise of new manufacturing technologies on the market, the OEM has had several concerns when deploying these solutions. First, the OEM has had to face obstacles created by a heterogeneous mix of production systems just as the MCM. The lack of common data interfaces and protocols has required additional time, resources, and expertise to navigate, and the OEM believes that it will need on-going support to maintain these technologies since its in-house expertise is relatively light. There are also significant cybersecurity concerns for the OEM, especially since the OEM would like to interact with its supply chain as well. If these issues are resolved, the OEM still faces data challenges created by the relatively small batch size. Like the MCM, the OEM has found it difficult to generate sufficient data for analysis and decision making, which again highlights the need for verification and validation tools.

USE CASE EXAMPLE

There were several shared themes observed during the case studies despite the noted differences between the three SME classifications. Perhaps least surprising of these themes was that many (if not all) SMEs believe that they fully understand their performance until they are confronted with real data and information from their systems. This process often motivated further introspection from the SME and generated a strong motivation to explore the opportunities presented by improved sensing, health management, and control. The initial interest tended to focus on relatively straightforward areas of performance, such as equipment utilization. This interest usually then grew into a desire to add detail and context that enables the SME to identify specific operational events and explain why these events occur. The state-of-the-art solutions in the field, such as the software described in the Introduction, have started to develop these types of capabilities. In addtion, other interests included prognostics and predictive maintenance and dynamic scheduling, which was often perceived as the natural use case for digital and PHM technologies for manufacturing. Several existing standards and technology efforts have started developing to support these areas. For example, standards, such as MTConnect, OPC UA, Automation ML, and MQTT, have started to generate enhancements that support machine-to-machine (M2M) communication, data interoperability, and other capabilities needed for prognostics and predictive maintenance and dynamic scheduling.

The themes described previously all highlight potential use cases that can be used to advance and develop digital and PHM technologies for manufacturing. Appropriate use cases are critical to generate reference datasets and protocols, test scenarios, and verification and validation tools that enable solution providers to address industry's needs and manufacturers to evaluate various technology alternatives. Six areas for potentially impactful use cases emerged from the case studies:

- Planning and scheduling support
- Maintenance planning and spare part provisions
- Request for proposals
- Resource budgeting (e.g., capital investments)
- Workforce augmentation
- Automation

Downloaded From: http://proceedings.asmedigitalcollection.asme.org/ on 09/27/2016 Terms of Use: http://www.asme.org/about-asme/terms-of-use

A general use case example that features several of the areas defined above is an automated workcell that accepts raw material and produces a finished part. The workcell could contain multiple machine tools for cutting operations and robots for pick-and-place operations. These components would be coordinated with each other based on the measured performance state of all components by an overarching control system. This control system would route materials dynamically based on the measured current state and performance of the system as well as input from design, engineering, suppliers, and other actors across the manufacturing enterprise.

To simplify the use case, the workcell would focus on one milling operation in a larger process chain. All of the machine tools would be identical three or five-axis computer numerical control (CNC) machining centers at varying stages of degradation. The machining centers would be of moderate age (five to eight years) and include a standard set of peripheral components common in CNC equipment, such as coolant and lubricant systems, cutting fluid systems, chip conveyors, tool crib, pallet changer, and multiple internal sensors for the control. Common faults and failures that we would expect include spindle or axis bearing failure, motor failure, tool breakage, and machine calibration errors. Only one robot would be used for pick-and-place within the workcell. The robot would require supporting hardware and software systems, such as a controller, end-effector, sensors, safeguards (e.g., light screens or pressure mats), and human interface. Even though robotic systems are typically robust, common faults and failures that we could expect include gear and motor failures.

The workcell would also interact with an operator and several external systems critical for its operations. One operator would be in charge of the entire workcell, but this operator's role would be primarily to ensure that the workcell maintains a predetermined level of performance. For example, the operator would conduct maintenance activities on all or a portion of the workcell when indicated by the control system. Solidworks and MasterCAM would be the CAD and CAM systems, respectively, used by the engineering support staff. E2 (or another similar software solution) would provide scheduling and MRP support. In addition, a simple MTConnect-enabled productivity solution would be deployed in the workcell that connects to operational information from the equipment controllers.

The performance of the workcell would be determined by a set of metrics and KPIs common to SMEs. Examples of metrics and KPIs include basic utilization and/or equipment availability, workcell throughput, workcell efficiency and/or conformance to estimation (i.e., actual to estimated cycle time), and rework rate. These metrics and KPIs could be calculated from a variety of data sources, including operational information from machine and robot controllers, engineering systems (e.g., CAD, CAM, and product lifecycle management systems), and additional shop-floor sensors. Further research would need to be conducted to verify the appropriateness of these data sources.

SUMMARY

The case studies conducted in this research highlight opportunities for and barriers to the deployment of digital and PHM technologies for SME manufacturers. Strong interest exists in the community, especially for basic equipment performance, but there is hope that advances in sensing, monitoring, and control will provide operational support that enables predictive maintenance and dynamic scheduling. Other potentially impactful areas for further research include maintenance planning and spare part provisions, request for proposals, resource budgeting, workforce augmentation, and automation. Large barriers remain, though, that can limit the deployment of digital and PHM technologies in manufacturing. Four barriers repeated by most of the SMEs interviewed for these case studies where:

- Lack of common data interfaces and protocols
- Lack of sufficient data to support analysis
- Lack of sufficient security tools to protect sensitive information and intellectual property
- Potential disruption to operations

While demonstration and clear return-on-investment are all necessary to educate industry about advanced manufacturing technologies, further research is needed to enable industry to overcome the barriers above and make full use of new digital and PHM technologies. Much of this research should focus on developing heterogeneous system-of-systems approaches that can connect various shop-floor systems together and with design and inspection. Advanced sensing and monitoring are needed to understand the highest-value data and information so that manufacturers avoid the challenges of big data (especially the volume and variety of data) and any disruption to operations. Reference datasets and verification and validation tools are needed to help develop tools that meet the needs to industry. New paradigms are needed that enable the use of generated intelligence to better control design and manufacturing processes. Finally, standardization is a critical part of ensuring that these technologies can be used successfully by all manufacturers. Appropriately defined use cases are needed to address these research questions. Such use cases will allow manufacturers to realize the full potential of digital and PHM technologies.

ACKNOWLEDGMENTS AND DISCLAIMER

The authors would like to acknowledge Ron Pieper, TechSolve, and Genedge Alliance for their exceptional support during these case studies. This paper would not be possible without the participation of the many SMEs involved in this effort. Certain commercial systems are identified in this paper. Such identification does not imply recommendation or endorsement by NIST. Nor does it imply that the products identified are necessarily the best available for the purpose.

Downloaded From: http://proceedings.asmedigitalcollection.asme.org/ on 09/27/2016 Terms of Use: http://www.asme.org/about-asme/terms-of-use

REFERENCES

[1] Inasaki, I. and Tönshoff, H. K., 2001, Sensors Applications: Volume 1 – Sensors in Manufacturing, Wiley, New York, NY, pp. 1-6.

[2] Lee, D. E., Hwang, I., Valente, C. M. O., Oliveira, J. F. G., and Dornfeld, D. A., 2006, "Precision Manufacturing Process Monitoring with Acoustic Emission," International Journal of Machine Tools and Manufacture, **46**(2), pp. 176-188.

[3] Liang, S., Hecker, R. L., Landers, R. G., 2004, "Machining Process Monitoring and Control: The State-of-the-Art," Journal of Manufacturing Science and Engineering, **126**(2), pp. 297-310.

[4] Helu, M. and Hedberg, T., 2015, "Enabling Smart Manufacturing Research and Development using a Product Lifecycle Test Bed," Procedia Manufacturing, **1**, pp. 86-97.

[5] Helu, M., Morris, M., Jung, K., Lyons, K., and Leong, S., 2015, "Identifying Performance Assurance Challenges for Smart Manufacturing," Manufacturing Letters, **6**, pp. 1-4.

[6] Evans, P. C. and Annunziata, M., 2012, "Industrial Internet: Pushing the Boundaries of Minds and Machines," General Electric.

[7] Drickhamer, D., Whitehead, C., and Walker, M., 2015, "The Industrial Internet of Things: Secrets to Finding ROI Today," Technical Seminar, IndustryWeek, http://event.lvl3.on24.com/event/10/99/53/2/rt/1/documents/resourceList1450194828762/webinar_sas2015_final.pdf, accessed 12/15/2015.

[8] Kalgren, P. W., Byington, C. S., Roemer, M. J., and Watson, M. J., 2007, "Defining PHM, a Lexical Evolution of Maintenance and Logistics," 2006 IEEE AUTOTESTCON – IEEE Systems Readiness Technology Conference Proceedings: Integrating Maintenance into the DoD Net-Centric Environment, IEEE, Anaheim, CA, pp. 353-358.

[9] Energetics Incorporated, 2015, "Measurement Science Roadmap for Prognostics and Health Management for Smart Manufacturing Systems," National Institute of Standards and Technology, Gaithersburg, MD.

[10] Gao, R., Wang, L., Teti, R., Dornfeld, D., Kumara, S., Mori, M., Helu, M., 2015, "Cloud-Enabled Prognosis for Manufacturing," CIRP Annals – Manufacturing Technology, **64**(2), pp. 749-772.

[11] Teti, R., Jemielniak, K., O'Donnel, G., Dornfeld, D., 2010, "Advanced Monitoring of Machining Operations," CIRP Annals – Manufacturing Technology, **59**(2), pp. 717-739.

[12] Albert, M., 2012, "MT Connect: Two Shops Share Their Experience," Modern Machine Shop, August 2012, http://www.mmsonline.com/articles/mt-connect-two-shops-share-their-experience, accessed 12/15/2015.

[13] Waurzyniak, P., 2015, "Why Manufacturing Needs Real-Time Data Collection," Manufacturing Engineering, October 2015, pp. 53-61.

[14] MTConnect Institute, 2015, MTConnect v. 1.3.1, http://www.mtconnect.org/standard?terms=on, accessed 12/15/2015.

[15] Size Standards Division, Office of Government Contracting and Business Development, 2009, "SBA Size Standards Methodology," U. S. Small Business Administration.

[16] Jin, X., Siegel, D., Weiss, B. A., Gamel, E., Wang, W., Lee, J., Ni, J., 2016, "The Present Status and Future Growth of Maintenance in US Manufacturing: Results from a Pilot Survey," Manufacturing Review, to appear.

Downloaded From: http://proceedings.asmedigitalcollection.asme.org/ on 09/27/2016 Terms of Use: http://www.asme.org/about-asme/terms-of-use

Development of Standard Test Methods for Evaluation of ROV/AUV Performance for Emergency Response Applications

Adam Jacoff and Kamel Saidi
National Institute of Standards and Technology
Intelligent Systems Division
Gaithersburg, Maryland, USA
kamel.saidi@nist.gov

Robert Von Loewenfeldt
South Carolina Law Enforcement Division
Columbia, South Carolina, USA
rvonloewenfeldt@sled.sc.gov

Yukio Koibuchi
University of Tokyo,
Tokyo, Japan
koi@k.u-tokyo.ac.jp

Abstract— This paper discusses the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) efforts to develop standard test methods for aquatic response robot performance. Different remotely operated vehicles (ROVs) and autonomous underwater vehicles (AUVs) were used to evaluate the test methods and the tests were refined accordingly. Experiments were conducted in order to evaluate the validity of the test methods. Results of those experiments as well as future work are discussed herein.

Keywords—ROV; AUV; underwater robot; test methods; performance; emergency response robot

I. Introduction

Remotely operated vehicles (ROVs) and Autonomous Underwater Vehicles (AUVs) have multiple emergency response applications such as bomb disposal, search and rescue, and disaster response. For example, ROVs and AUVs were used to conduct underwater cleanup and victim recovery following the 2011 earthquake and tsunami in Japan [1]. Bomb squads, search and rescue teams, and disaster response teams need to know the performance of the ROVs and/or AUVs that they own or plan to purchase in order to understand their capabilities and to match those capabilities with the scenarios in which they will be deployed.

A few standards exist for ROVs for industrial applications [2, 3], but these only relate to ROV interfaces and a few basic measures of performance, primarily within the petroleum and natural gas industries. Although a few guides exist [4] there are currently no standard tests to evaluate ROV or AUV performance for emergency response applications.

The National Institute of Standards and Technology (NIST), in cooperation with other organizations, has been leading efforts by the Robot Task Group under the ASTM Sub-Committee E54.08 on Operational Equipment for Homeland Security Applications. The task group has published 15 international standards for response robots [5] to date and these standards have been replicated by dozens of organizations worldwide to measure and evaluate response robot capabilities. The standards address critical needs by helping to inform response robot procurement and deployment decisions with statistically significant robot-capabilities data for a variety of mission-essential tasks. These standards also help guide robot manufacturers toward innovations that answer responder needs while encouraging hardening of developmental systems. To date, ASTM E54.08.01 standards have been used to specify more than $50M worth of response robot procurements for firefighters, bomb squads, and soldiers. These standards are now also beginning to enhance operator training by supporting newly developed measures of operator proficiency.

Although some of the above standards may be applied to land, aquatic, or aerial response robots, the primary focus of the subcommittee so far has been on terrestrial (or ground) robots. The work presented in this paper may be adopted by ASTM E54.08 or by another standards committee or organization.

II. Background

NIST is presently developing a suite of tests that can be used to evaluate basic capabilities of ROVs and AUVs. This paper discusses the subcommittee's past and present efforts to develop test methods for aquatic response robots. The tests include, among others, tasks that are intended for measuring the ROV/AUV's cutting, inspection, station keeping, object retrieval, object placement, sonar resolution, visual acuity, and mapping capabilities. In addition, the maximum thrust and payload carrying capacities are also being considered.

ROV/AUV requirements for search and rescue applications were developed based on input from the

This work was partially sponsored by the US Department of Homeland Security (DHS) Science and Technology Directorate, Test, Evaluation & Standards Division.

Jacoff, Adam; Saidi, Kamel; Von Loewenfeldt, Robert; Koibuchi, Yukio.
"Development of Standard Test Methods for Evaluation of ROV/AUV Performance for Emergency Response Applications."
Paper presented at the OCEANS 2015 MTS/IEEE Conference, Washington, DC, Oct 19-Oct 22, 2015.

user community [6]. The requirements include: structural inspection, leak localization/mitigation, object (body) recovery, water traverse, rapid current station keeping, payload delivery, and object recovery. Bomb squad requirements are somewhat more specialized since ROVs/AUVs must deal with underwater explosives. Bomb squad ROV/AUV requirements were also developed based on user feedback.

In addition to the above requirements, the objective of these underwater test methods, as well as for all the test methods developed for ground and aerial robots, is to provide quick and easy ways to measure capabilities that anybody can replicate and practice to evaluate their own ROV/AUV.

III. Descriptions of the Test Methods and Apparatuses

The proposed test methods and apparatuses described below were developed at NIST and during field exercises. These test methods and apparatuses are still evolving and are considered early prototypes. Changes to initial designs are discussed in Section VI.

A. Bollard Thrust

The bollard thrust test method measures the zero-speed pulling capability of an ROV (i.e., it is not affected by drag or other factors). This is equivalent to the maximum thrust of the ROV. This simple test is important because robot manufacturers often provide values for maximum thrust on their specifications sheets based on theoretical calculations. Instead, the simple apparatus described below measures the ROV's maximum thrust directly.

The test apparatus consists of a stationary mounting point, a cable redirected through a pulley, and a digital force gauge connected to the stationary end of the cable (Fig. 1). The apparatus can be secured to the side of a water tank or to a dock for testing.

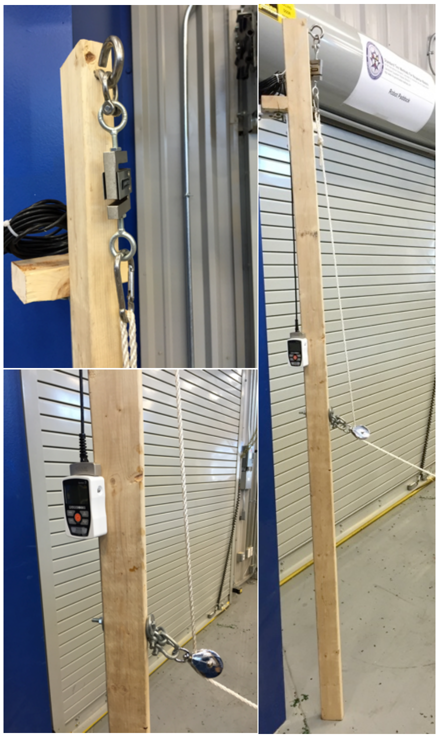
B. Inspection/Station Keeping

The inspection (or station keeping) test method measures an ROV's ability to maintain its position in the water under specific conditions (e.g., turbidity or current). This is accomplished by providing a set of targets that the ROV has to inspect (Fig. 2). Each target consists of a series of nested acuity optotypes of decreasing size. The ROV must attempt to identify the orientation of the smallest optotype possible in each target. ROVs with better station-keeping capabilities should be able to perform this task faster.

C. Visual Acuity

The visual acuity test method is equally important in open air as it is under water (where visibility is measurably more impaired). This test consists of placing several charts (Fig. 3), with specific acuity optotypes on them, at a certain distance from an ROV and evaluating the ability of the ROV/operator to read the charts through the ROV's interface.

Fig. 1. The bollard thrust apparatus.



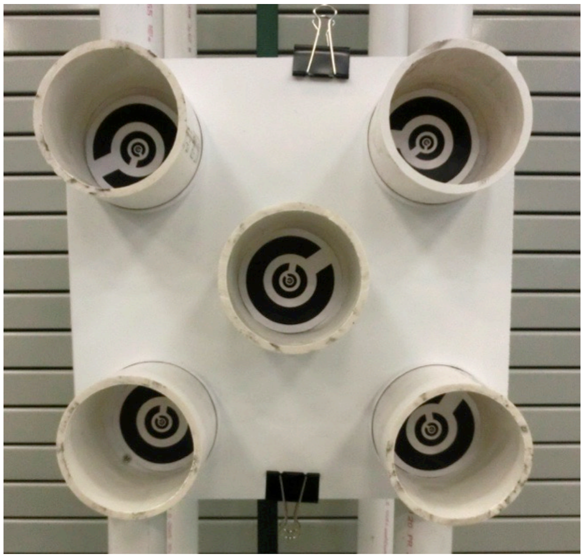
D. Mapping

Underwater mapping of a harbor (e.g., after a hurricane) is a very important task, especially because there are few other options. The same mapping fiducial concept that is used for ground robots [7] was adapted and submerged underwater.

The initial apparatus that was developed consisted of plastic cylinders with aluminum wings that bisected the cylinder (Fig. 4). The apparatus was held up in the water using buoys (orange spheres in Fig. 4) at the top and weights at the bottom. The apparatus depicted in Fig. 4 also incorporated visual acuity targets on the wings in order to simultaneously test mapping and visual acuity.

The cylinder with wings makes for a very distinctive shape when scanned and mapped and its location and orientation should be readily apparent in the sonar image. They can be deployed in single height or double height configurations depending on the water depth available. When they were originally deployed in the double height configuration, the wings were offset 90 degrees from one another. This was changed in subsequent revisions of the apparatus.

Fig. 2. The inspection/station keeping apparatus.



The apparatus is buoyed from the top and anchored to the bottom with two separate anchors so as to minimize translation or rotation while floating submerged below the water's surface.

Map evaluations using these mapping fiducials for ground robots include metrics for coverage, consistency, local accuracy, and global accuracy [7] that can be directly applied to underwater map evaluations.

E. Sonar Resolution

The sonar resolution test method measures the resolving capability of a sonar sensor, which is the prevailing navigation sensor on underwater robots (given that visual sensors are so hindered by water conditions such as turbidity).

The initial sonar resolution apparatus that was developed consisted of a 1 m square sheet of aluminum with a series of 9 holes, of 3 different sizes, cut out of it (Fig. 5). The apparatus is buoyed from the top and anchored to the bottom with two separate anchors so that it does not translate or rotate while floating submerged below the water's surface. Placing the apparatus at a certain standoff distance from a wall would then show reflections from the aluminum and the wall (which would also allow us to determine the sonar's angle of incidence as well as its range resolution). The sizes of the holes could be varied based on the expected resolution of the sonar.

Another design of the sonar resolution apparatus consists of simple 3D geometric objects (such as cubes, cylinders, and pyramids) of varying sizes. The objects are placed anywhere within an ROVs environment or in predetermined orientations (Fig. 6).

Fig. 3. The visual acuity apparatus.

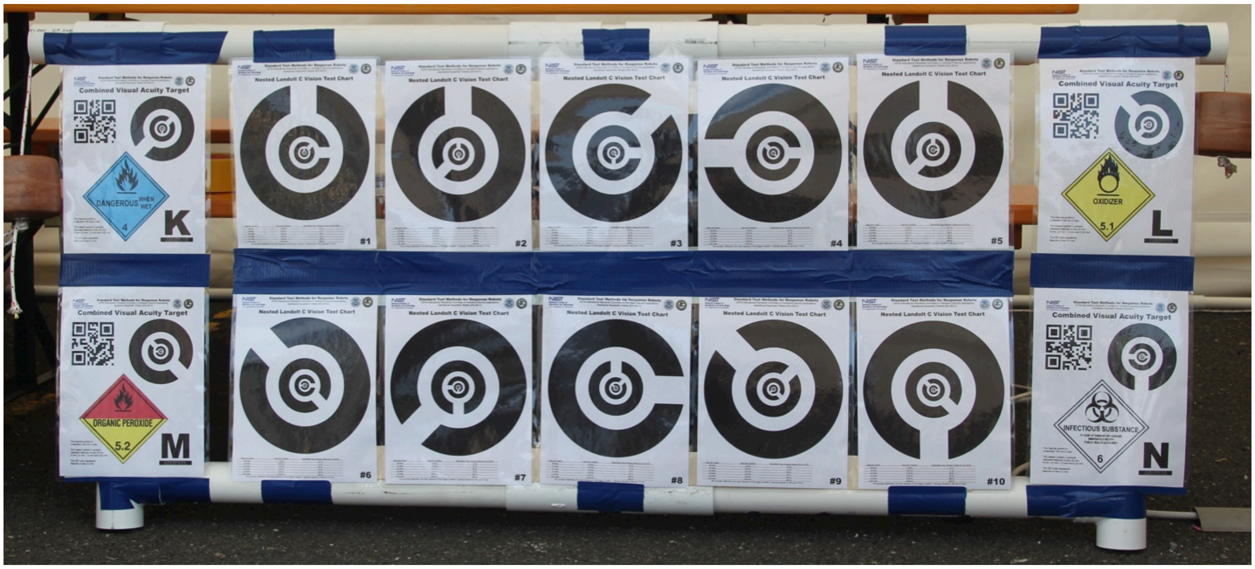
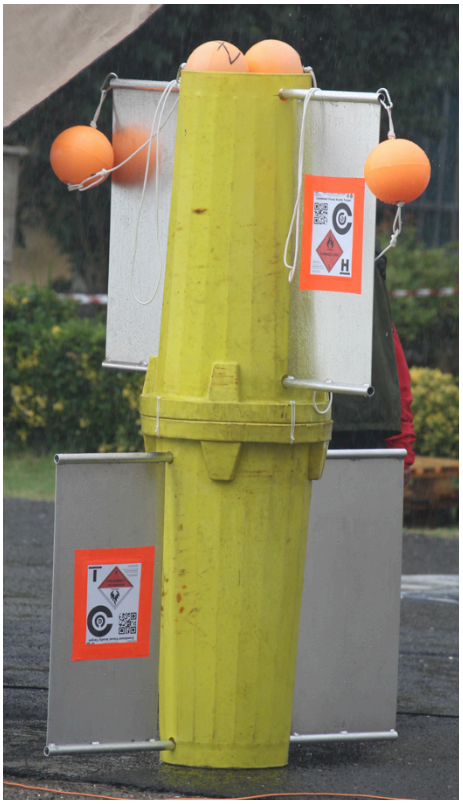


Fig. 4. A double-height underwater mapping fiducial with plastic cylinders and aluminum wings.



F. Rope Cutting

The rope-cutting test method measures the ROV's ability to cut through rope or cable of different materials and thicknesses and in different orientations.

The initial rope-cutting apparatus consisted of 2 different sizes of rope with 10 repetitions of each size, 5 horizontal and 5 vertical cuts. Each rope was equipped with a small shape-/color-coded buoy to indicate success and timing at the surface. Two separate anchors and a floatation buoy centered above the apparatus ensured that it didn't change position and orientation once placed, and that it floated upright (Fig. 7).

Fig. 5. The flat sonar resolution apparatus.

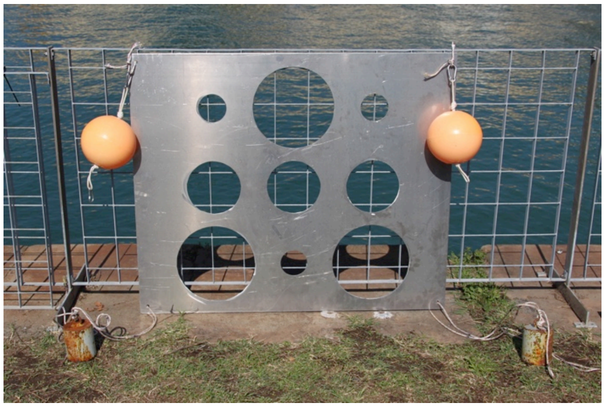


Fig. 6. The three-dimensional sonar resolution apparatus.

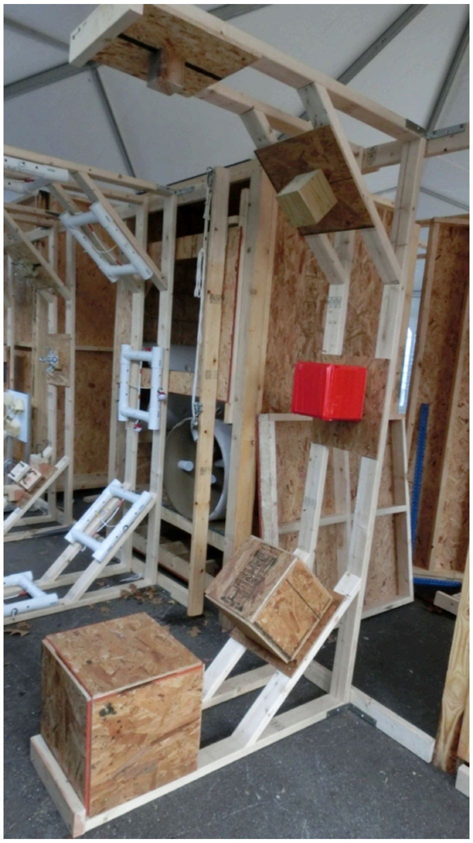
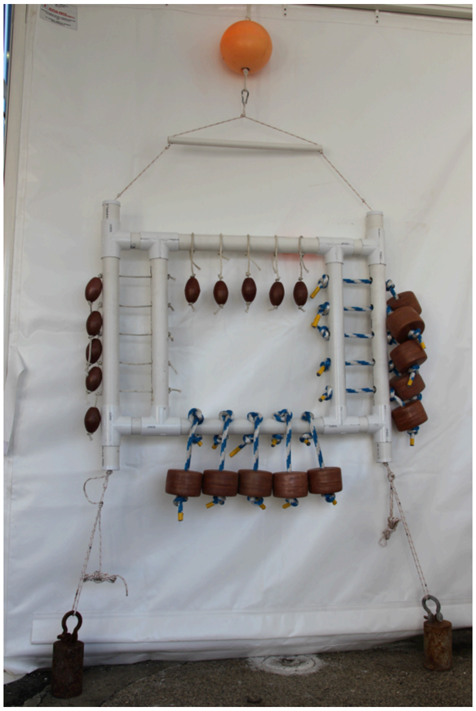


Fig. 7. The rope-cutting apparatus.



G. Rod Cutting

The rod-cutting test method measures the ROV’s ability to cut through rods of different materials and thicknesses and in different orientations.

The initial rod-cutting apparatus consisted of wooden dowels placed in an apparatus that accommodated two trials of 10 repetitions, 5 horizontal and 5 vertical cuts (Fig. 8). Much like the rope-cutting apparatus, the rod-cutting apparatus also included a buoy attached to each rod.

H. Hooking

The hooking test method measures the ROV’s ability to deploy a carabiner (or similar device) to hook onto an object underwater. This type of task is often conducted in search and rescue scenarios.

The hooking apparatus consists of 5 U-bolts arranged in different orientations as shown in Fig. 9. The ROV must attempt to hook the carabiner onto all 5 U-bolts.

I. Soft Grab

The soft grab test method is similar to the hooking test method in that it measures the ability of the ROV to deploy a tool that can attach to something underwater. In the case of the soft grab test method, the tool is an alligator clip (Fig. 10) and the object to hook onto is a soft target that can be made out of foam or cloth (Fig. 11). This type of task is meant to simulate the retrieval of a bag or a victim.

Fig. 8. The rod-cutting apparatus.

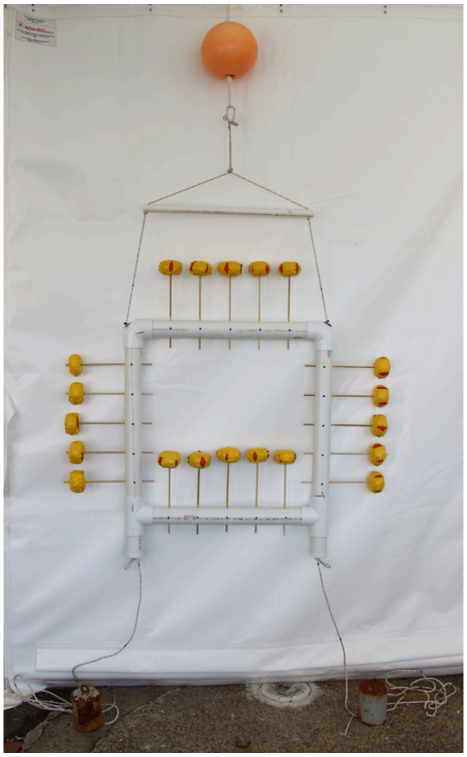
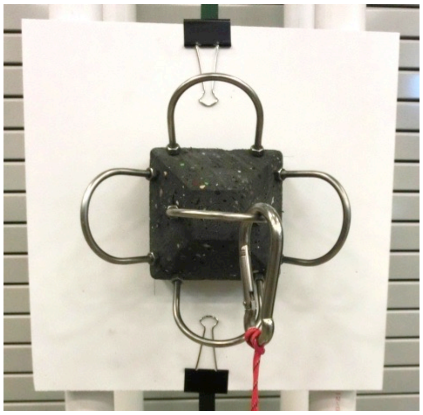


Fig. 9. The hooking apparatus.



J. Grasp, Surface, Swim, and Place

The grasp, surface, swim, and place test measures the ability of an ROV to retrieve an object, surface with the object in its gripper, swim across the surface a certain distance, and then place the object back on the bottom.

The apparatus consists of a weight, 2 target areas (from which to pick and in which to place the weight), and 2 pylons that mark the distance over which the ROV must swim at the surface (Fig. 12).

Fig. 10. The foam version of the soft grab apparatus.

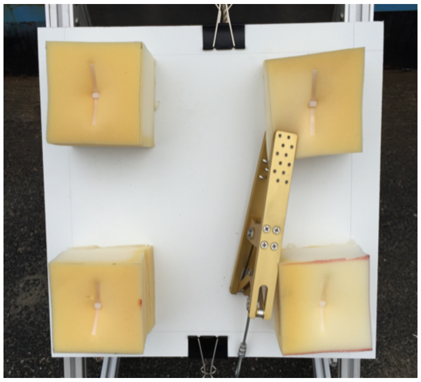


Fig. 11. The cloth version of the soft grab apparatus.

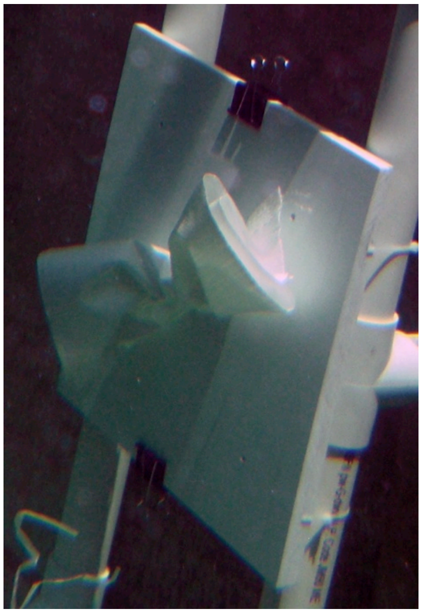
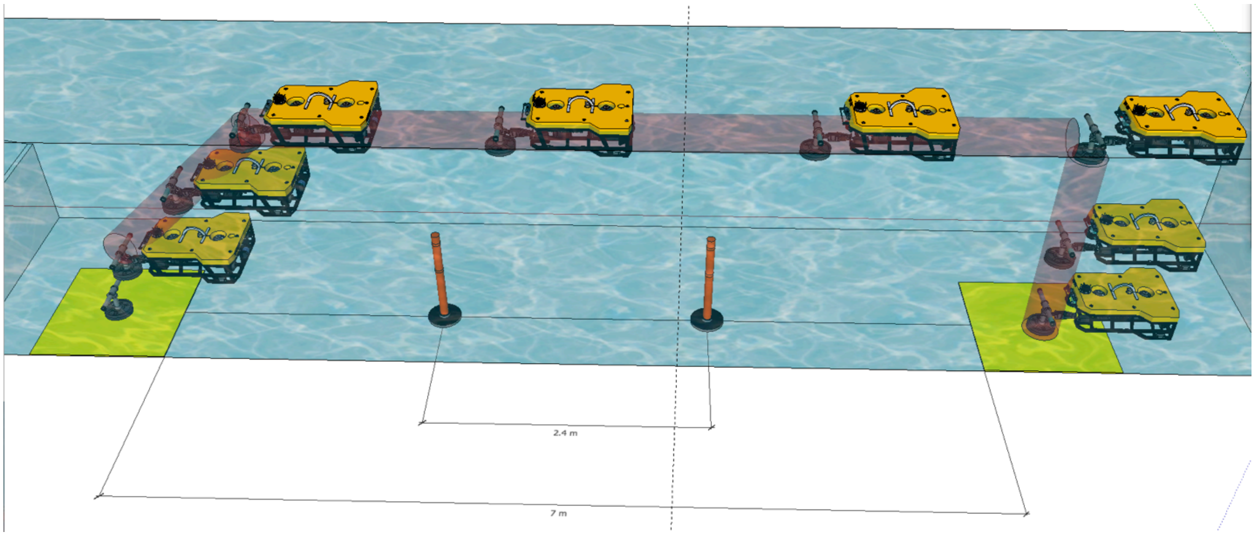


Fig. 12. The grasp, surface, swim, and place apparatus showing a simulated test trajectory.



K. Disruptor Placement

The disruptor placement test method measures the ROV's ability to place a magnetized disruptor (an explosive ordinance defeat device) close to an IED (improvised explosive device) attached to a ship's hull.

The apparatus consists of a 40 cm square thin sheet of metal affixed to a plastic board of similar size (Fig. 13). The disruptor is simulated by a short (25 cm) metal pipe with 2 magnets attached to it. The IED is simulated by a plastic box with a single magnet attached to it.

IV. Common Apparatus Carrier Design

Five of the test apparatuses (inspection/station keeping, rope and rod cutting, hooking, soft grab, and disruptor placement) described in the previous section are implemented onto a common apparatus carrier (Fig. 14). The common carrier is made out of polyvinylchloride (PVC) pipe[1] and allows 5 test apparatuses to be mounted onto it at the same time and at 5 different angles (Fig. 15). This provides the ROV with the opportunity to conduct the same test in 5 different orientations, which not all ROVs are capable of achieving.

[1] The original common carrier was constructed out of wood (Fig. 6), but it was found to be too buoyant. The second design was constructed out of aluminum, but it was found to be relatively expensive to replicate.

Fig. 13. The disruptor placement apparatus.

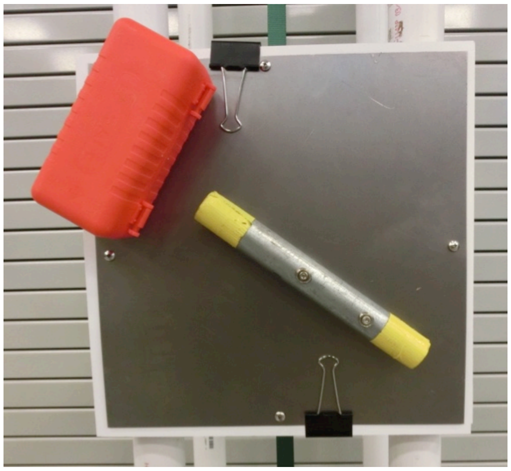


Fig. 14. The common apparatus carrier.

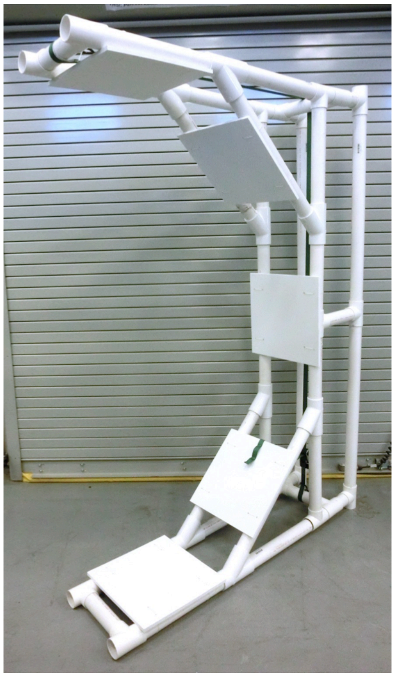
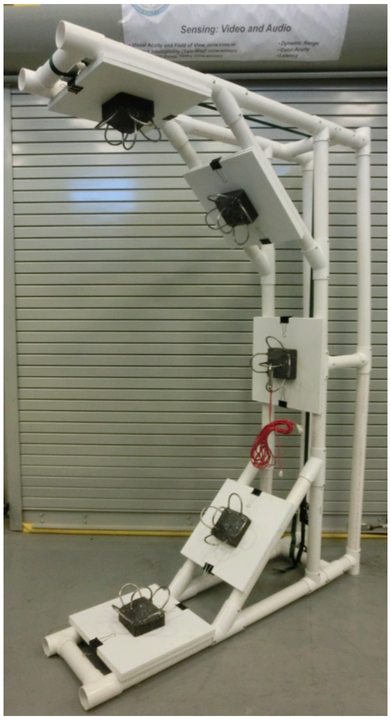


Fig. 15. The common apparatus carrier with 5 hooking tasks.



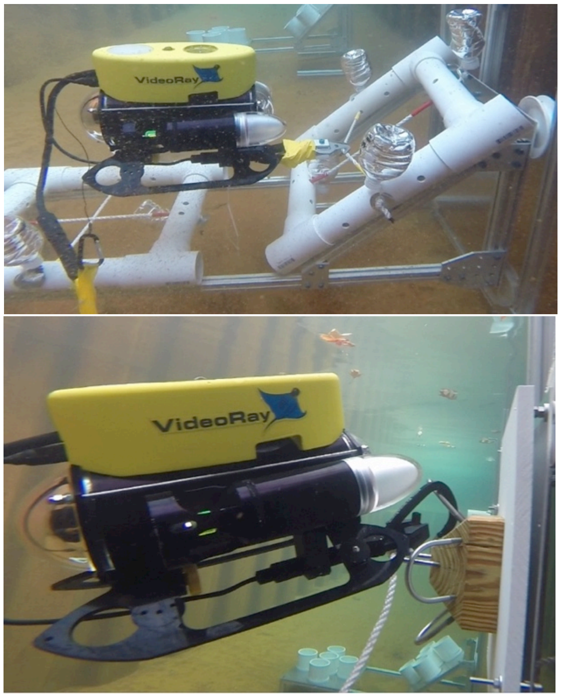
V. Validation Exercises

The majority of the test methods and corresponding apparatuses described above were deployed at multiple locations over the past year. The locations include a 70 m^3 tank at NIST in Gaithersburg, Maryland (Fig. 16); a harbor at the 2014 Eurathlon competition, in La Spezia, Italy (Fig. 17 and Fig. 18); a 70 m^3 tank at the San Diego Fire-Rescue Training Facility in San Diego, California (Fig. 19); and a 70 m^3 tank at the Defense Advanced Research Projects Agency (DARPA) Robotics Challenge (DRC) Finals Expo in Pomona, California (Fig. 20).

Earlier versions of some of the apparatuses were also deployed at Disaster City in College Station, Texas in 2011 (Fig. 21).

During the above exercises, the primary objectives were to validate the practicality and effectiveness of the apparatuses, to start developing procedures for conducting the tests, and to understand the limitations and challenges of the environments into which the apparatuses were deployed.

Fig. 16. An ROV performing a rope-cutting task (top) and a hooking task (bottom) in the NIST tank[2].

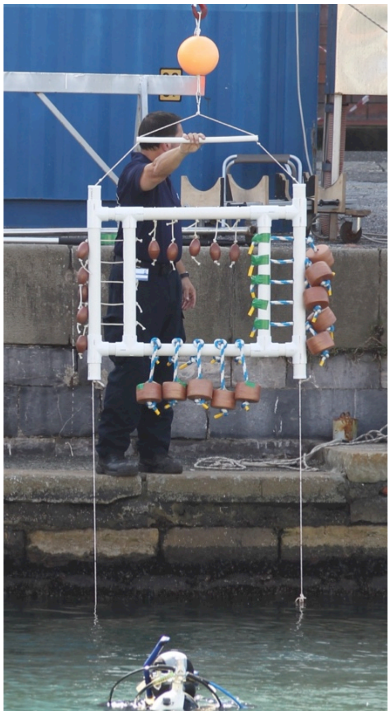


VI. Lessons Learned

Several improvements to and variations of the test methods and apparatuses came about as the result of the validation exercises described above. Some of these changes are summarized below:

- Changed from single-task apparatus that provides only one task orientation at a time to a common carrier with 5 simultaneous task orientations for easier statistically significant testing.
- Changed from a wood common carrier design to an aluminum design with rollers for each task (seen in Fig. 16) for ease of task administration (e.g., replacing cut ropes) and reducing apparatus buoyancy.
- Changed from rollers to slides for ease of fabrication.
- Changed from aluminum common carrier design to PVC for reducing cost and ease of replication.
- Changed from foam soft grab objects to cloth for reducing apparatus buoyancy.
- Changed from multiple sizes of U-bolts, for the hooking task, to one medium-size U-bolt for reducing complexity and as a starting baseline.
- Changed from single height mapping fiducials to double height for increased visibility in deeper water.
- Changed from 90° offset wings in the double height mapping fiducials to non-offset wings for reducing complexity in the sonar data (Fig. 22).
- Changed from plastic to metal cylinders in the mapping fiducials for better sonar reflection (Fig. 22).
- Made various refinements to the common carrier design including quick task attachment using binder clips and different methods of securing the carriers inside a tank.
- Decided that all tests should be conducted under ideal water visibility conditions as a baseline and that turbidity should be measured during each test.
- Decided to implement current to increase station-keeping difficulty.
- Changed from an outboard boat engine (Fig. 23) to submersible pumps (Fig. 24) for generating current to reduce safety concerns and for finer current control.

Fig. 17. A rope-cutting task consisting of 20 tasks in 2 different diameter ropes being deployed in a harbor at the 2014 Eurathlon competition.



[2] Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

Fig. 18. A combined mapping fiducial and visual acuity target. Top left inset shows a view from an AUV camera while the top right inset shows the output of a sonar system with the target circled in white. The bottom picture shows the target being deployed in a harbor at the 2014 Eurathlon competition.

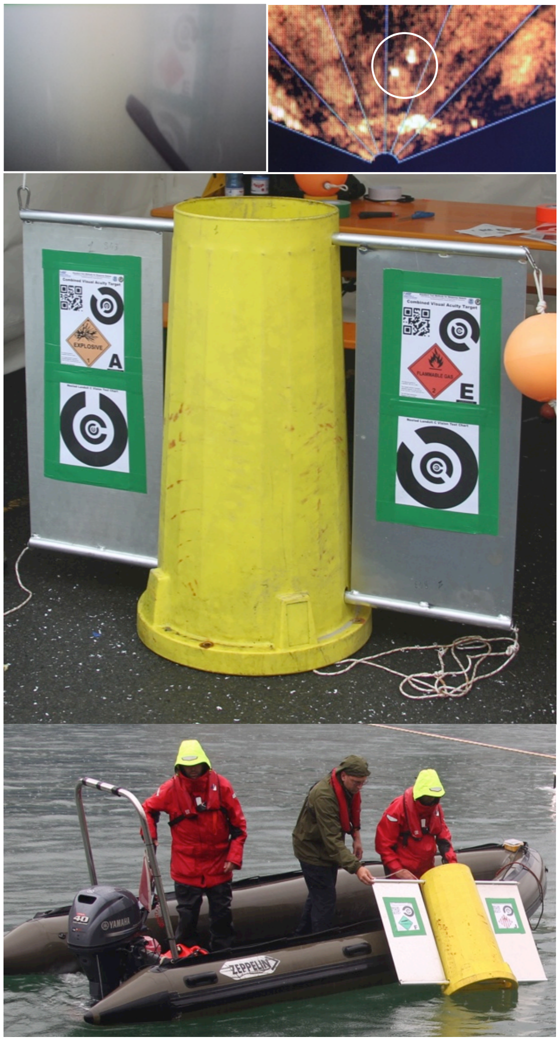


Fig. 19. ROV tests deployed in a tank at the San Diego Fire-Rescue Training Facility.

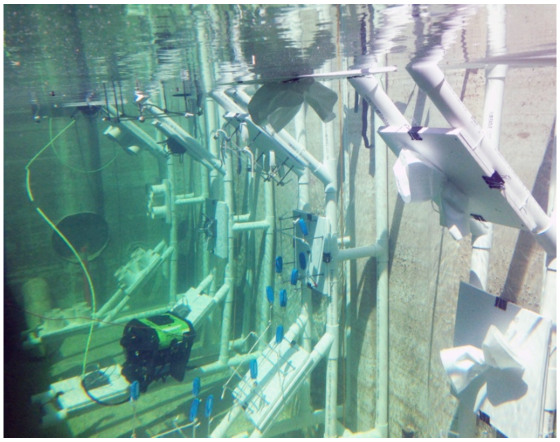


Fig. 20. An ROV performing an inspection task in a tank at the DRC Finals Expo.

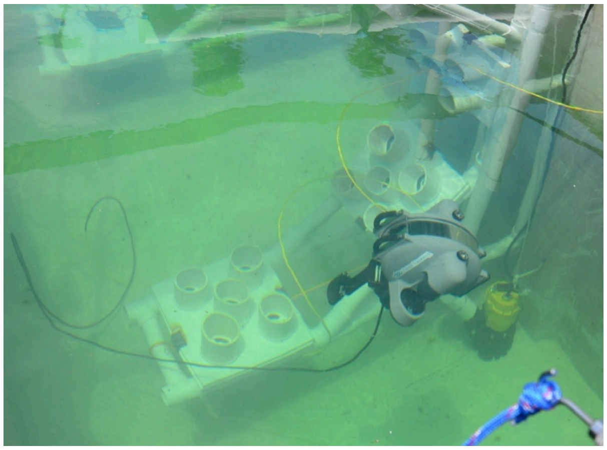
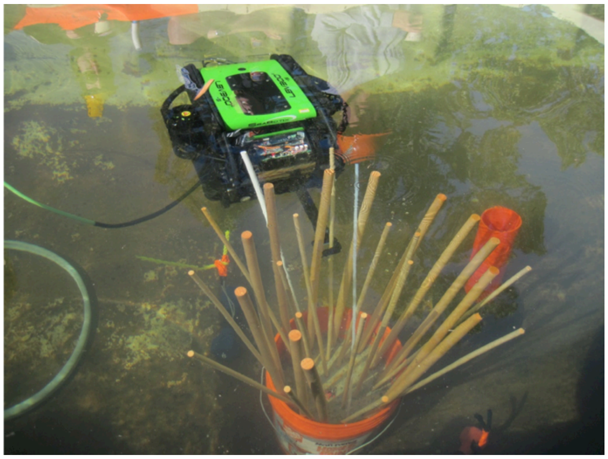


Fig. 21. An ROV performing a rod-cutting task in an early implementation of the apparatus at Disaster City.



VII. Conclusions and Future Work

Several apparatuses for testing ROV/AUV basic performance have been developed and demonstrated. These tests are a first step in developing standard test methods for evaluating ROV/AUV performance. Based on several validation exercises conducted over the past year, the tests were deemed to be challenging enough for many currently available ROVs. The tests do not cover all aspects of ROV/AUV performance, but they are a good first step at quantifying performance.

Future work includes additional exercises to validate the test methods already developed. Specifically, more validations are needed for tests that some small ROVs are not able to complete (such as the grasp, surface, swim, and place and the disruptor placement tasks).

Current apparatuses will also continue to be refined to make them easier and cheaper to implement. In addition, the steps involved in conducting these tests will be further developed into more formal procedures.

Furthermore, although testing ROV/AUV basic capabilities is good for understanding performance, sometimes conducting tasks found in actual scenarios presents unforeseen challenges and helps operators and manufacturers better understand their system's capabilities. To that end, more realistic scenarios will be developed and deployed to assess an ROV's performance after it has successfully navigated the set of basic tests.

Fig. 22. Design for a new double-height mapping fiducial using steel drums.

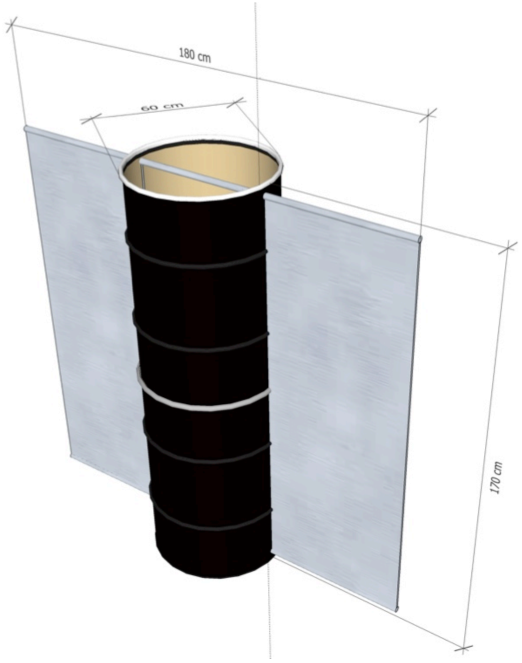


Fig. 23. An outboard boat engine mounted inside a shallow water tank to generate current.

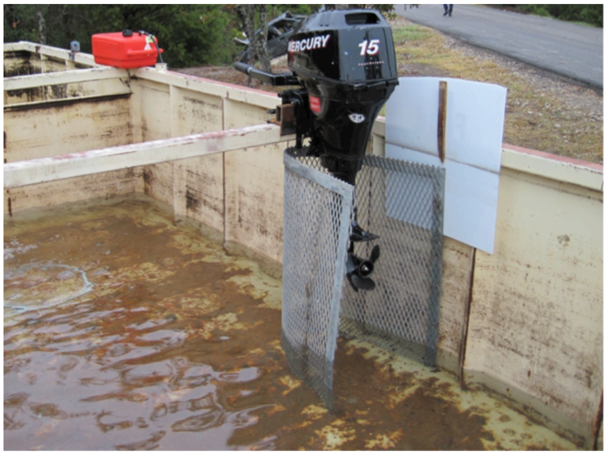
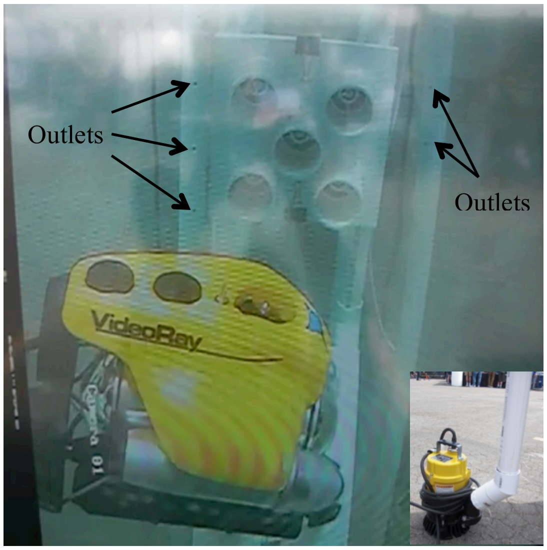


Fig. 24. Current generation using a submersible pump (inset) in front of an inspection/station keeping apparatus inside a tank.



Finally, the water current generation methods will be refined to generate stronger flows as needed; turbidity will be varied in a controlled fashion to assess how an ROV's performance is affected by reduced visibility; and new test methods and apparatuses will be developed as the need for them arises.

References

[1] Robin R. Murphy, Karen L. Dreger, Sean Newsome, Jesse Rodocker, Brian Slaughter, Richard Smith, Eric Steimle, Tetsuya Kimura, Kenichi Makabe, Kazuyuki Kon, Hisashi Mizumoto, Michinori Hatayama, Fumitoshi Matsuno, Satoshi Tadokoro, and Osamu Kawase, "Marine heterogeneous multirobot systems at the great Eastern Japan Tsunami recovery," Journal of Field Robotics, Vol. 29, No. 5, pp. 819-831, September 2012.

[2] ISO 13628-8:2002, Petroleum and natural gas industries -- Design and operation of subsea production systems -- Part 8: Remotely Operated Vehicle (ROV) interfaces on subsea production systems, The International Organization for Standardization (ISO), Geneva, Switzerland.

[3] NORSOK U-102:2012, Remotely operated vehicle (ROV) services, Edition 2, September 2012, Standards Norway, Lysaker, Norway.

[4] Committee F41 on Unmanned Maritime Vehicle Systems (UMVS), http://www.astm.org/COMMIT/SUBCOMMIT/F41.htm, Accessed: August 10, 2015.

[5] ASTM Subcommittee E54.08 on Operational Equipment for Homeland Security Applications: http://www.astm.org/COMMIT/SUBCOMMIT/E5408.htm, Accessed: August 10, 2015.

[6] Messina, Elena R. and Jacoff, Adam S., "Performance Standards for Urban Search and Rescue Robots," Proceedings of the SPIE Defense and Security Symposium, Orlando, FL, USA, 04/17/2006 to 04/21/2006.

[7] Sören Schwertfeger, Adam Jacoff, Chris Scrapper, Johannes Pellenz and Alexander Kleiner, Evaluation of Maps using Fixed Shapes: The Fiducial Map Metric, 2010, In Proc. of the Int. Workshop on Performance Metrics for Intelligent Systems (PerMIS), 344-351.

Proceedings of the 2015 Winter Simulation Conference
L. Yilmaz, W. K. V. Chan, I. Moon, T. M. K. Roeder, C. Macal, and M. D. Rossetti, eds.

TOWARDS A VIRTUAL FACTORY PROTOTYPE

Sanjay Jain

The George Washington University
2201 G Street NW
Funger Hall, Suite 415
Washington, DC- 20052, USA

David Lechevalier
Jungyub Woo
Seung-Jun Shin

Systems Integration Division
Engineering Laboratory
National Institute of Standards and Technology
Gaithersburg, MD – 20899, USA

ABSTRACT

A virtual factory should represent most of the features and operations of the corresponding real factory. Some of the key features of the virtual factory include the ability to assess performance at multiple resolutions and generate analytics data similar to what is possible in a real factory. One should be able to look at the overall factory performance and be able to drill down to a machine and analyze its performance. It will require a large amount of effort and expertise to build such a virtual factory. This paper describes an effort to build a multiple resolution model of a manufacturing cell. The model provides the ability to study the performance at the cell level, machine level, or the process level. The benefits and limitations of the presented approach and future research directions are also described.

1 INTRODUCTION

Progress towards achieving the vision of smart manufacturing systems requires the abilities to conduct detailed analytics on current performance, to evaluate potential future courses of actions, and to set the course that best leads towards the goals. These abilities can be termed respectively as diagnostic, predictive, and prescriptive analytics. Diagnostic analytics assesses past-and-current performance and cause–and-effect relationships among major control factors and performance metrics. Predictive analytics evaluates future performance of a system operating under selected policies and forecasted requirements, such as demand scenarios. Prescriptive analytics helps develop future courses of actions using approaches such as optimization and combined simulation-optimization. Efforts to move towards smart manufacturing thus need to be supported by diagnostic, prescriptive and predictive analytics (Shao, Jain, and Shin 2014).

Jain and Shao (2014) proposed the virtual factory, which is a high-fidelity simulation of the manufacturing system to support data analytics. The term virtual factory has been used with multiple meanings in the research and professional literature. We utilize the definition of the virtual factory as "an integrated simulation model of major subsystems in a factory that considers the factory as a whole and provides an advanced decision support capability." Other terms used to describe the concept with minor variations include digital factory, virtual copy, and virtual plant model. The latter two terms have been used in the description of the recent Industrie 4.0 concept by Mario et al. (2015). They define cyber physical systems (CPS) as a key component of Industrie 4.0 because they utilize virtual copies of the physical world to support decentralized decision making.

Jain, Sanjay; Lechevalier, David; Woo, Jungyub; Shin, Seungjun.
"Towards a Virtual Factory Prototype."
Paper presented at the Winter Simulation Conference, Huntington Beach, CA, Dec 6-Dec 9, 2015.

The virtual factory concept encompasses the ability to analyze the manufacturing system at any desired level of detail - just as one would do for a real factory. One should be able to focus on 1) a single process step and analyze the performance of the associated equipment, 2) a particular line or department in the system, or 3) the factory as a whole. The virtual factory concept is represented in Figure 1. The figure shows models of manufacturing system at multiple levels of resolution extending from factory level at the top to device level at the bottom. These models should be integrated vertically across the hierarchy and horizontally with input data sources and output data analytics systems. Please see Jain and Shao (2014) for more details of the concept and the figure.

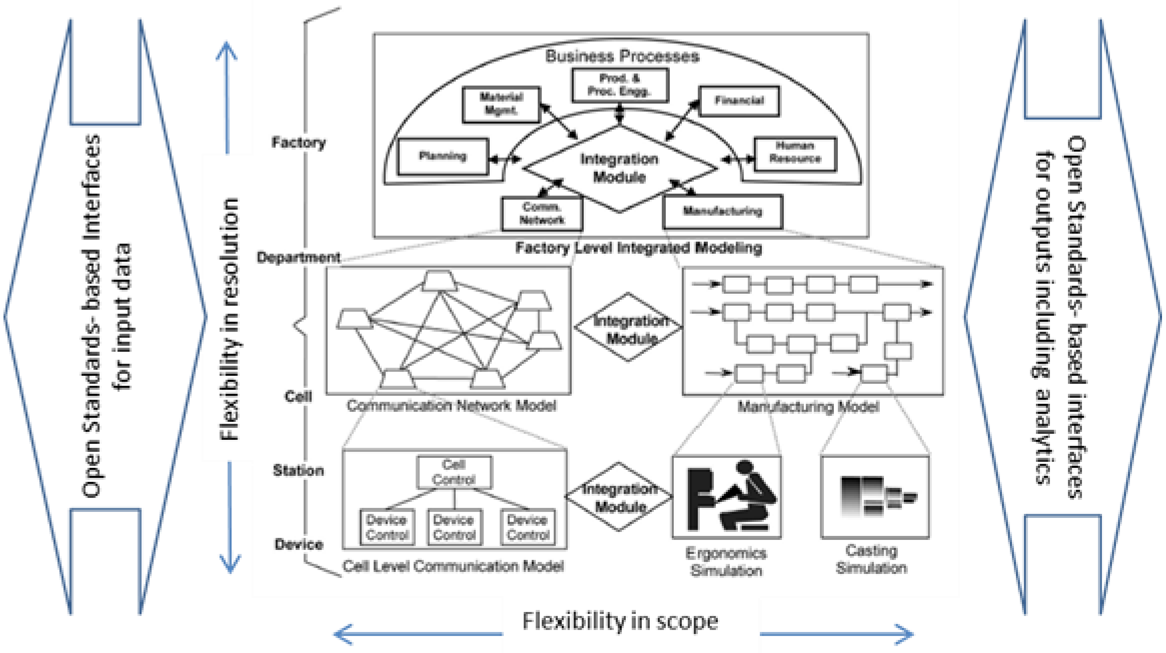


Figure 1: Virtual Factory concept (adapted from Jain and Shao 2014).

Developing virtual factories that correspond to real factories can be a large undertaking particularly if each such virtual factory is custom developed. One way, and perhaps the only way, to realize the virtual factory concept is via “crowd sourcing.” That is, a number of researchers need to contribute to build the models of sub-systems and atomic components in a way that they can be integrated to realize the concept. The models should be generic with the capability to be customized based on data describing the sub-systems and atomic components. Interested researchers should come together to 1) define an overall open architecture supported by relevant standards and 2) develop open modules that can be integrated to realize a specific virtual factory. Such an effort can take several years to come to full fruition. In our view, however, this capability can be built in stages by targeting more common manufacturing system configurations first. Even partial implementations of the virtual factory can be useful to industry. Indeed, industry has been using models of individual sub-systems to support manufacturing system design and operations as evidenced by papers presented in this conference over the years. Efforts such as Industrie 4.0 appear to be taking a similar approach for an even wider scope.

The groundwork to support any such scope includes defining, and exploring the feasibility of, the key aspects of the virtual factory concept. The brief description above suggests that any kind of feasibility checking requires multi-resolution modeling, which is the ability to model parts of a system at varying levels of detail. For example, one should be able to model a machine of interest in detail at the unit level or as part of a higher level system. Our research goal is to build a prototype of a virtual factory that can be used to assess the feasibility of any proposed key aspect. This will allow other researchers to assess the feasibility of their proposed, key aspects of the concept.

This paper represents a small step towards building a complete virtual factory prototype by exploring what capabilities that prototype needs to estimate the feasibility of multi-resolution modeling. Our research used a limited scenario - a small job shop with a single manufacturing cell comprising four turning machines. Our virtual prototype captures this scenario at three levels of detail. The top layer, the cell, has a model can that tracks the processing of each part as a single block of time. Typically, a cell model is implemented in a discrete event simulation (DES). At the machine level, each machine can be modeled at a greater granularity level of detail to 1) track the granular movements needed to process the part and 2) predict characteristics such as temperature and energy use. A machine model is implemented using the agent-based simulation (ABS) paradigm. At the process level, the physics of the process is modeled using physics equations coded in Java.

The next section of the paper provides a brief literature review. Section 3 presents the proposed approach for developing the virtual factory and for the multi-resolution modeling for the small job shop model. The implementation of the small job shop model with the three levels of detail and identified issues are discussed in section 4. Section 5 concludes the paper with discussion of next steps.

2 LITERATURE REVIEW

This section briefly reviews the recent literature in relevant areas, which include virtual factory, multi-resolution modeling, and hybrid simulation.

2.1 Virtual Factory

Jain and Shao (2014) provided a brief overview of virtual-factory literature. A few additional efforts employing the virtual-factory concept have been reported since then. Yang et al. (2015) emphasize the use of virtual reality for collaborative development of virtual factory. They present three application scenarios: production-system, production-cell, and workstation levels. The granularity of detail varies from one level to another. For, example, information about cutting tools and workpieces is taken account at the workstation level but not at the cell level. The three applications reported by Yang et al. (2015) do not appear to have the flexibility of combining different levels of details in the same model; and, thus, the effort has not fully implemented multi-resolution modeling.

Mourtzis et al. (2015) report on the increasing use of simulation in conjunction with digital manufacturing. The combination of simulation and digital manufacturing will lead towards a capability that is close to virtual factory per the definition used in this paper. Terkaj and Urgo (2015) describe a Virtual Factory Data Model (VFDM) to support the development of the virtual-factory model. They also describe a connector that automatically generates a simulation model based on the VFDM description. All these efforts appear to be aiming for the similar goal of realizing the vision of virtual factory while addressing different aspects. The aspect of multi-resolution modeling, the focus of this effort, does not appear to have been addressed in these efforts.

2.2 Multi-Resolution Modeling

Multi-resolution modeling appears to have received more attention in the context of combat simulation than in the context of manufacturing. Hong and Kim (2012) identify two major challenges in multi-resolution modeling: seamless data aggregation and disaggregation, and dynamic replacement of models at different resolutions. They develop a specification to address these challenges and show its application in an air combat scenario. Guan et al. (2012) propose a framework for digital-factory technology that includes both multi-level modeling and multi-resolution simulation. They utilize a distributed simulation framework to integrate simulations of process, plant layout, and supply chain. They demonstrated the

Jain, Sanjay; Lechevalier, David; Woo, Jungyub; Shin, Seungjun.
"Towards a Virtual Factory Prototype."
Paper presented at the Winter Simulation Conference, Huntington Beach, CA, Dec 6-Dec 9, 2015.

use of this framework in a case study that addresses the integration of a material handling simulation with a virtual reality model for static layout analysis.

Jain et al. (2013) utilized multi-resolution modeling of a supply chain. The high-level, supply-chain model is developed using a system dynamics simulation (SDS) paradigm with the ability to execute one of the manufacturing nodes at more detail using discrete event simulation (DES). The effort reported in this paper seeks to implement the idea within the virtual factory context with integrated modeling of cell and equipment levels.

2.3 Hybrid Simulation

Multi-resolution modeling often involves modeling different levels of abstraction using different simulation paradigms and thus can be viewed as hybrid simulations. For example, as mentioned above Jain et al. (2013) utilized SDS at the supply-chain level and DES at the factory level. Venkataswaran et al. (2006) used a similar SDS-DES hybrid simulation set up to plan operations to support vendor managed inventory. Hermann et al. (2011) combined discrete event simulation to model manufacturing processes with a continuous simulation to model the energy flows for planning manufacturing systems with consideration of environmental impact. Fakhimi et al. (2014) utilized a hybrid of agent-based simulation (ABS) and DES for strategic planning and simulation analytics of health care services. In their work, the two simulations interact to improve the performance of the system. The effort reported in this paper also utilizes an interaction between ABS and DES to implement multi-resolution modeling.

3 APPROACH

The approach is discussed in two sub-sections. First, the overall proposed approach for creating virtual factories is discussed. This is followed by discussion of the approach used for implementing multi-resolution modeling in a small prototype.

3.1 Overall Approach for Virtual Factory

Developing a full scale virtual factory will be difficult for most organizations to take on by themselves. We propose an approach that allows multiple participants – individual, groups, and organizations to develop modules that can be integrated to create the virtual factory. This approach would first require development of an open architecture based on standards that allows integrating modules for modeling virtual factories. The Industrie 4.0 effort mentioned in Section 2 includes the goal of developing virtual versions of real factories through a large coordinated effort (Mario, Tobias, and Boris 2015). It appears to be targeting a standard architecture and thus may provide an opportunity to integrate other independently developed modules.

The capability to develop virtual factories will be realized primarily using software. This presents an opportunity to develop the capability iteratively starting from a prototype and successively adding capabilities. The needed concepts, standards, and interfaces can be tested as corresponding capabilities are developed. As suggested earlier, such iterative development can be done by multiple participants on various sub-systems and components of the virtual factory related to their interest and applications.

Development of software by multiple participants in an open community requires common understanding and agreement on several aspects including scoping of constituent modules, selection of standards, and selection of applicable ontologies. The alternatives for each aspect need to be carefully explored and considered. It will help significantly, and may indeed be required, to develop prototypes exploring the alternatives, for at least the major aspects, to capture the issues involved and associated advantages and disadvantages. Prototypes would also help communicate the long-term vision and serve to capture feedback from the end users. An initial push towards development of the virtual factory can occur via developments of prototypes exploring different aspects by multiple interested researchers and associated discussions at forums such as simulation conferences.

The development reported in this paper is an initial prototype that explores the idea of multi-resolution modeling in the context of a virtual factory. It considers three levels of resolution, a process level, a machine level and a manufacturing cell level. The three levels are implemented in the same simulation software to keep the focus on the issues in integrating multiple levels of resolution. Implementing the three levels in different simulation software would have required a mechanism to synchronize executions such as distributed simulation and would have added another layer of complexity.

3.2 Approach for Multi-Resolution Modeling

Multi-resolution modeling (MRM) requires the capability to execute different parts of a model at different levels of resolution. Note, that hierarchical levels in a manufacturing context have been defined for decades (e.g., Jones and Mclean 1986; Williams 1994) and have been recently captured in standards such as IEC 62264-3 (ISO 2013). Unfortunately it appears that there isn't one widely accepted standard definition of such levels. The hierarchical levels are generally defined with the idea of control and may not correspond with the software applications that implement that control. To gain acceptance from industry users, the levels in virtual factory will need to be set up to match those standards that have wider acceptance than others. The virtual factory will also need to have the flexibility to modify level definition to match hierarchies defined in other official and de-facto standards.

The lower levels of the manufacturing control hierarchy may be defined to include a manufacturing cell level, followed successively by machine/equipment and process levels. The prototype reported in this paper represents these three levels with modeling of 1) physics of the process with time modeled in milliseconds, 2) operations at machine level, with events occurring every few seconds, and 3) functions at the cell level, with events occurring in the range of every few minutes.

In addition to the time granularity, the three levels are different in other ways. The implementation of the three levels makes certain scoping decisions. The machine level operations treat a batch as a collection of individual parts and track batch loading, individual part set-up, execution of turning process on individual parts, followed by part unload and repeating of this cycle for all parts in the batch. A batch unload step is modeled after all parts have been processed. While most of the actions are modeled in discrete event paradigm, the actual turning process is represented in continuous time in the process level model. At the manufacturing cell level, the batch is treated as a single item and processing times are modeled accordingly using discrete event paradigm.

An alternate implementation may model times for processing of individual part features at the machine level and time for processing the entire part at manufacturing cell level. The prototype thus allows exploring and highlighting some of the scoping options. Alternate assumptions and/or selections can be made in other prototype efforts or even in future version of this prototype based on inputs from other researchers and practitioners.

The three levels have been implemented using a bottom-up approach. The process-level model was developed first and calibrated against real machines that were instrumented to capture the measures of interest. The machine-level models was developed next and validated against the real machine data. The validated virtual-machine models were executed multiple times and the resulting batch processing times were captured. The batch processing times are computed using the start of batch set-up to end of batch unload. Therefore, it includes multiple cycles of individual part set-up, processing and unload times. These batch process times are used to model the machine operations at the manufacturing cell level. The user is given an option to model selected machines at the machine level while the rest of the cell can be modeled at the manufacturing cell level. Of course, the user can run the entire cell with all machines modeled at machine level of detail and they can run the entire cell with all machines at manufacturing cell level of detail.

The current prototype represents batch processing times with the assumption of the times being normally distributed. The collected individual batch times are analyzed to determine the means and standard deviations and recorded for use in manufacturing cell level execution. In future, more advanced curve fitting analysis will be used to identify and select distributions that most closely represent the collected times.

4 IMPLEMENTATION

This section describes the implementation of the prototype using a simulation environment. The process level model is briefly discussed first. The development of the machine level model using agent-based simulation (ABS) is discussed next together with the capabilities to execute it in summary or detailed mode. Next the development of the manufacturing cell level using discrete event simulation is presented that integrates ABS model and the capability of execution in summary or detailed mode.

4.1 Process-Level Model

The process-level model is an implementation of the virtual-turning-machining model that was developed to simulate machining process based on process planning data (Shao, Jain, and Shin 2014). It utilizes discretized continuous equations that represent the physics of the process dynamics and kinematics of a machine tool. It models machine components such as the spindle motor and servo motors, parameters such as depth of cut and feed rate to determine cutting forces and the resulting energy and time consumption. The inputs to the simulator are machine parameters and process planning data in STEP-NC format (ISO 2007). The outputs are generated in format compliant with the MT-Connect standard (MTConnect 2014) and include parameters such as time and energy consumption. For the current MRM prototype, only the time values are passed to the machine level model. In near future, other parameters in particular the energy consumption will be passed and aggregated at higher levels.

The process-level model was originally developed in C++ and transformed to Java for ease of integration with the machine level model developed in AnyLogic (Grigoryev 2015). Process level simulations are typically available in CAD/CAM software. However, in this prototype an independently developed module was used to allow implementation of the three levels within one simulation environment.

4.2 Machine-Level Model

The machine-level model has been implemented as an agent utilizing the Agent-based Modeling constructs in AnyLogic. Specifically the model has been implemented using the Statechart construct of the Agent palette in AnyLogic to mimic the modeled states of the machine as shown in Figure 2. The default machine state is the *Idling* state. During the simulation, the machine stays in this state as long as it does not get any batch to process. As soon as a batch arrives (represented by transition 1 in Figure 2), the machine goes to the *batchSetup* state that models the machine set up for processing the batch. The following sequence of states depends on the level of detail being modeled.

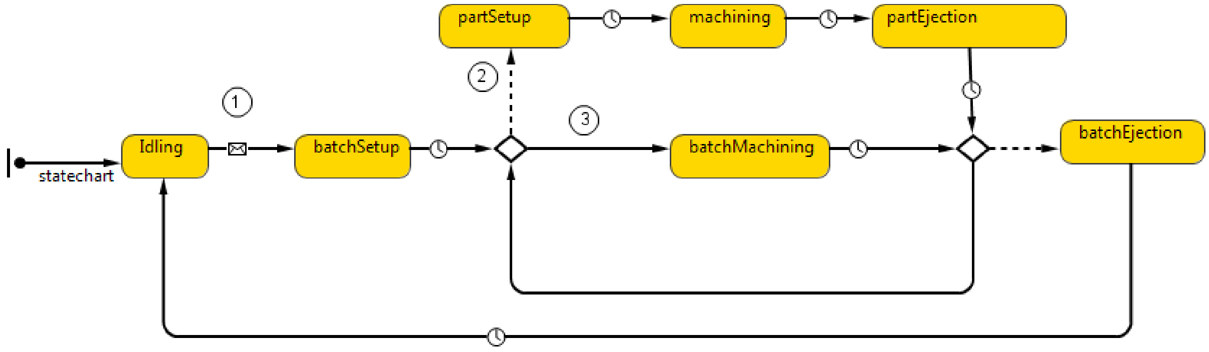


Figure 2: State chart for the machine level model.

If the machine is running in detailed mode (transition 2) representing the machine level of detail, the next state is the *partSetup* state where the machine sets up each part in order to execute needed operations. The corresponding functions configure machine parameters depending on the material that has been set up in the previous state. These parameters include feed rate and spindle speed. Following the completion of *partSetup,* the state transitions to *machining* state that represents the metal-cutting process. After the machining state, the machine goes to the *partEjection* state that models unloading the part. The logic loops through the states as many times as there are parts in the batch. The times to process one part, that is the transition from beginning of the *partSetup* state to the end of the *partEjection* state are recorded and used to calculate the average and standard deviation of the part processing time.

The process-level model in section 4.1 models the detailed steps for all the states that have corresponding STEP-NC instructions. The process level determines the times required for execution of the STEP-NC instructions and passes it back to the statechart to model the passage of time. The structure allows modification or even replacement of the process model without affecting the machine level or the higher-level models. The STEP-NC source file is customized using the machine parameter values generated in the *partSetup* state. With this file as input, a specific function of the process-level model models the cutting process and determines the machining time to process one part of the batch.

If the machine is running in the summary mode, representing the manufacturing cell level, the state chart goes directly to the *batchMachining* state (transition 3). This path summarizes the other path by modeling the processing of the entire batch at one time using the average and standard deviation of the individual part-processing times. The concept of Central Limit theorem is used to aggregate the individual part process times into batch process times. Generally, minimum 30 data points are recommended for application of Central Limit theorem (Berenson, Levine, and Krehbiel 2002) and this criteria will be implemented in the model. This is admittedly a simple approach. Future versions of the prototype may allow more options such as empirical representation and fitted continuous distributions. Finally the last state is the *batchEjection* state, when the batch unload step is modeled. The time for processing successive batches are recorded and can be used for analysis such as aggregating them for representing the process at a further lower resolution such as line or plant level.

4.3 Manufacturing Cell-Level Model

The manufacturing cell-level model has been developed using discrete event simulation capability of AnyLogic as shown in Figure 3. The manufacturing cell is composed of four turning machines that are represented using the process modeling library provided in AnyLogic.. A S*ource* node generates part batch arrivals following a uniform distribution between 6 and 8 per hour. Each batch can contain ten to fifteen identical parts. Three part types are considered with the exact same geometry but with different material. The material for the parts can be aluminum, steel or titanium. The batch is sent to a *Queue* and then to an object called *SelectOutput* that chooses the machine to which the batch is routed. The S*electOutput* utilizes the shortest queue dispatching rule for this decision.

The machines are represented using a *ResourcePool* object (called Turning001, Turning 002, etc) in the figure. A *ResourcePool* object can comprise of a number of resources and allows the facility of the resources being agents. In this model, each *ResourcePool* includes a turningMachine agent as the resource. This structure allows linking the manufacturing cell-level model represented using the process modeling library to the machine-level model represented using the agent library. Again, the machine-level model can be replaced easily without impacting the manufacturing cell-level model.

The processing of the batches by machines is modeled using the sequence of *Seize, Delay*, and *Release* objects. The *Seize* objects have been named as machines Turning1, Turning2, etc. in Figure 3. The arrival of the batch at the machine, i.e., on the *Seize* step, triggers the arrival of the batch on the *batchSetup* state of the corresponding machine agents state chart discussed in the preceding sub-section. The processing of the batch is modeled in the machine using the agent-based model. During this time, the batch is held in the *Delay* object at the cell level. Once the unit has processed the full batch, the agent sends the signal to release the batch from the *Delay* object. The batch is released and its exit from the cell is modeled via the *sink* object. The corresponding machine agent goes to the idling state at the agent-based model level. The user can specify the choice of resolution level for each machine at the manufacturing cell level using the checkbox on the left. Each checkbox is associated with one machine. Depending on the choice made by the users, the batch will choose either the machine level of detail (detailed) path or the manufacturing cell level of detail (summary) path in the state chart described in the previous sub-section.

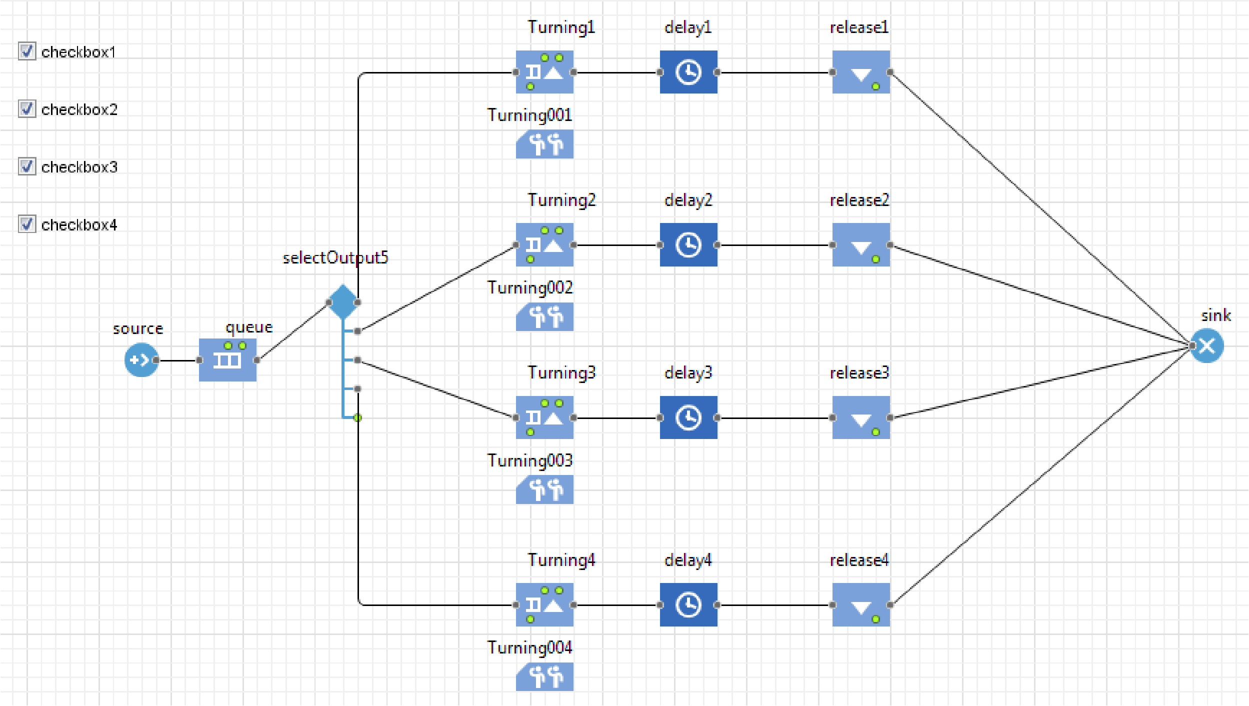


Figure 3: Manufacturing cell level model represented using discrete event simulation.

4.4 Execution at Multiple Resolution Levels

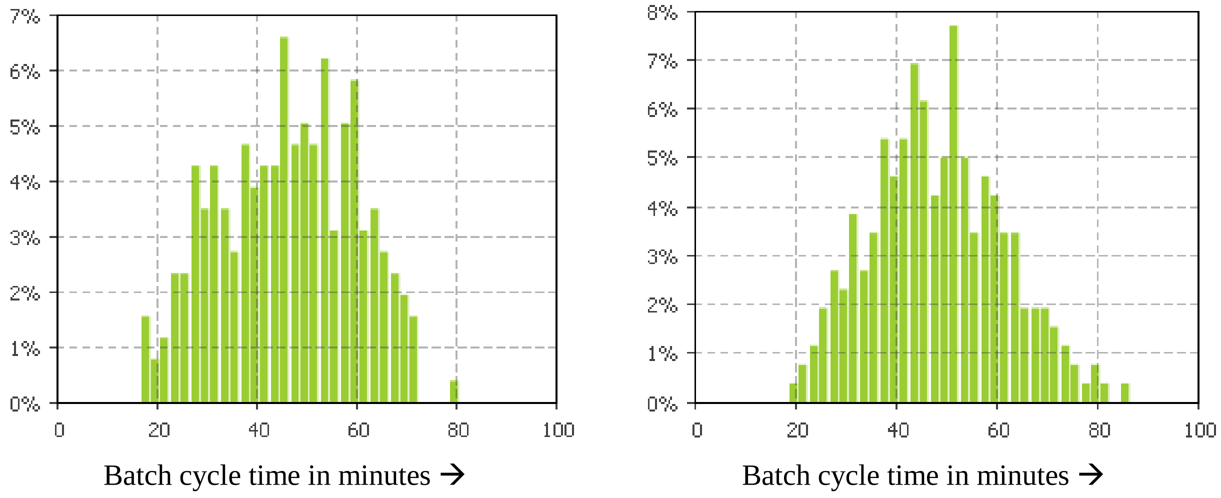
The implementation of the prototype model allows executing the simulation at multiple resolution levels as listed below.

- The manufacturing cell can be modeled with all machine models executing at manufacturing cell level, that is, with processing modeled for entire batch at a time.
- The manufacturing cell can be modeled with all machine models executing at the machine level, that is, with processing modeled at individual part level complete with determination of time and energy consumption based on the physics of the process.
- The manufacturing cell can modeled with user-selected machines executing at the manufacturing cell level and other machines executing at the machine level of detail.

The capability of executing the model at multiple resolution levels is available via the checkboxes provided at the manufacturing cell level. The checkboxes give the user the option of either executing at the default machine level of detail (detailed) or the manufacturing cell level of detail (summary).

The current implementation of the model is set up to allow the selection of the resolution level of detail only after at least one batch using a given material has been processed. The first batch is always executed at the machine level of detail. The execution of the first batch of parts is used to capture the data for individual part processing and generate the parameters for use in the distribution of the batch processing times. For instance, if the first batch contains aluminum parts, the checkbox would be unavailable. As soon as a second batch of aluminum parts arrives to the machine, the check box would be available to be selected. Again, this is a simple approach used for this prototype. In future versions, the model may be executed with machine level of detail for longer runs and data collected for aggregation and use in execution with multiple resolution level. Capabilities can be developed to set up the length of the run based on the desired width of the confidence interval for the individual part processing times.

The models at multiple resolution levels should be valid representations of the underlying real world phenomena based on the purpose of the model. Such validation will require comparison with the real world data. The performance of the models with selected measures will need to be compared and their accuracy for the desired purpose evaluated following procedures such as those described by Sargent (2014). The underlying model of the turning process has been previously validated for its prediction of energy consumption (Shao, Jain, and Shin 2014). While a detailed validation is planned as the next step in this prototype-building exercise, an initial comparison of results from execution at the two levels of details shows agreement on batch cycle times, which was one of the desired goals. The batch cycle time is calculated as the time between the arrival at the source and the exit at the sink. The comparison runs used a 1-week (40-hours) simulation time and the same arrival patterns of batches for the two detail levels. The random seed was initialized for reproducibility of the results for both the models. The outputs of the system differed slightly with 260 batches completed when executed at the machine level of detail and 258 batches completed at the manufacturing cell level of detail. A two tailed z-test at the 95 % confidence level indicated that the two batch cycle time samples were not statistically different. Figure 4 shows the distribution of batch cycle times generated for the two runs. The x-axis represents the time in minutes while the y-axis represents the percentage of batches that are in corresponding range of time.



(a) Manufacturing cell level of detail

(b) Machine level of detail

Figure 4: Distributions of batch cycle times with all machines at (a) the manufacturing cell level of detail and (b) the machine level of detail.

5 CONCLUSION

This paper reports on an initial prototype to explore the feasibility of multi-resolution modeling in the context of virtual factory. By design, this first step took an approach that avoided other complicating factors. For example, the models at different resolution were within the same simulation environment and thus the complexity of implementing distributed simulation was avoided. Similarly, simple approaches were used for aggregation of data from machine level to manufacturing cell level and for setting up the multiple resolution execution. The exercise indicated that multiple resolution modeling is feasible at least in this simplified environment.

Future work will focus on iteratively adding capabilities and complexities. The initial step reported in this paper utilized machine level models for turning machines. Additional machining processes will be added in the near term and a range of process models may be considered in future. A process model for milling machines is nearly complete and will be the next one to be integrated in the prototype. The initial step reported here focused on use of a simulation environment that allows modeling at multiple resolutions. An alternate approach of representing the detailed level using tools specifically developed for process simulations is being explored. Integration with separate tools will require the use of a distributed simulation set up with its associated complexities. The current prototype used standards for the input and output for the machine level model. For future versions, additional interfaces based on standards will be developed. The factory data may be imported using the Core Manufacturing Simulation Data (SISO 2012) standard and the outputs may be generated using Business To Manufacturing Markup Language (B2MML; MESA 2013) standards. Also, the current implementation used ad-hoc terminology for the three levels of details. Standard terminology and scope of levels of resolution in manufacturing modeling will be explored for future iterations. The preceding are some of the ideas for enhancements under considerations. The actual iterative enhancements will be driven by the overall Smart Manufacturing System program that this initiative is a part of at the National Institute of Standards and Technology (NIST).

DISCLAIMER

No approval or endorsement of any commercial product by NIST is intended or implied. Certain commercial software systems are identified in this paper to facilitate understanding. Such identification does not imply that these software systems are necessarily the best available for the purpose.

ACKNOWLEDGMENTS

Sanjay Jain's work on this effort has been sponsored under the cooperative agreement no. 70NANB13H158 between the NIST and George Washington University. The work described was funded by the United States Government and is not subject to copyright.

REFERENCES

Berenson, M. L., D. M. Levine, and T. C. Krehbiel. 2002. *Basic Business Statistics: Concepts and Applications,* 8th ed., p. 249-251. New Jersey: Prentice Hall.

Fakhimi, M., A. Anagnostou, L. Stergioulas, and S. J. E. Taylor. 2014. "A Hybrid Agent-Based and Discrete Event Simulation Approach for Sustainable Strategic Planning and Simulation Analytics." In *Proceedings of the 2014 Winter Simulation Conference*, edited by A. Tolk, S. D. Diallo, I. O. Ryzhov, L. Yilmaz, S. Buckley, and J. A. Miller, 1573-1584. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Grigoryev, I. 2015. *AnyLogic 7 in Three Days: A Quick Course in Simulation Modeling.* 2nd edition.

Guan, Z. L., C. J. Wang, Y. F. Wu, and X. Y. Shao. 2012. "A Framework of Digital Factory System Using Multi-Resolution Simulation." *Applied Mechanics and Materials* 159:12-17.

Herrmann, C., S. Thiede, S. Kara, and J. Hesselbach. 2011. "Energy Oriented Simulation of Manufacturing Systems – Concept and Application." *CIRP Annals - Manufacturing Technology* 60(1): 45-48.

Hong, S.-Y., and T. G. Kim. 2012. "Specification of Multi-Resolution Modeling Space for Multi-Resolution System Simulation." *Simulation: Transactions of the Society for Modeling and Simulation International* 89(1):28–40.

ISO. 2007. *ISO 10303-238:2007. Industrial ~~a~~Automation ~~s~~Systems and ~~i~~Integration.* International Standards Organization (ISO)..

ISO. 2013. *IEC 62264-1:2013. Enterprise-control ~~s~~System ~~i~~Integration -- Part 1: Models and ~~t~~Terminology*. International Standards Organization (ISO).

Jain, S., S. Sigurðardóttir, E. Lindskog, J. Andersson, and B. Johansson. 2013. "Multi-Resolution Modeling for Supply Chain Sustainability Analysis." In *Proceedings of the 2013 Winter Simulation Conference*, edited by R. Pasupathy, S.-H. Kim, A. Tolk, R. Hill, and M. E. Kuhl, 1996-2007. Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc.

Jain, S., and G. Shao. 2014. "Virtual Factory Revisited for Manufacturing Data Analytics." In *Proceedings of the 2014 Winter Simulation Conference*, edited by A. Tolk, S. D. Diallo, I. O. Ryzhov, L. Yilmaz, S. Buckley, and J. A. Miller, 887-898. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Jones, A. T., and C. R. McLean. 1986. "A Proposed Hierarchical Control Model for Automated Manufacturing Systems." *Journal of Manufacturing Systems* 5(1):15-25.

Mario, H., P. Tobias, and O. Boris. 2015. "Design Principles for Industrie 4.0 Scenarios: A Literature Review." Working Paper No. 01 / 2015, Technische Universität Dortmund, Dortmund, Germany.

MESA 2013. *Business To Manufacturing Markup Language Release Notes Version 6.0 – March 2013.* MESA International, Chandler AZ.

Mourtzis , D., N. Papakostas, D. Mavrikios, S. Makris, K. Alexopoulos. 2015. "The Role of Simulation in Digital Manufacturing: Applications and Outlook." *International Journal of Computer Integrated Manufacturing* 28(1): 3-24.

MTConnect. 2012. "Part 1-Overview and protocol, Version 1.2.0" MTConnect Institute (2012).

Sargent, R.G. 2014. "Verifying and Validating Simulation Models." In *Proceedings of the 2014 Winter Simulation Conference*, edited by A. Tolk, S. D. Diallo, I. O. Ryzhov, L. Yilmaz, S. Buckley, and J. A. Miller, 118-131. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Shao, G., S. Jain, and S.-J. Shin. 2014. "Data Analytics using Simulation for Smart Manufacturing." In *Proceedings of the 2014 Winter Simulation Conference*, edited by A. Tolk, S. D. Diallo, I. O. Ryzhov, L. Yilmaz, S. Buckley, and J. A. Miller, 2192-2203. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

SISO 2012. *SISO-STD-008-01-2012: Standard for Core Manufacturing Simulation Data – XML Representation*. Simulation Interoperability Standards Organization, Orlando, F L.

Terkaj, W., and M. Urgo. 2015. "A Virtual Factory Data Model as a Support Tool for the Simulation of Manufacturing Systems." *Procedia CIRP* 28:137–142.

Venkateswaran, J., Y. J. Son, A. T. Jones, and J. Min. 2011. "A Hybrid Simulation Approach to Planning in a VMI Supply Chain." *International Journal of Simulation and Process Modeling*, 2(3/4):133-149.

Williams, T. J. 1994. "The Purdue Enterprise Reference Architecture." *Computers in Industry* 24(2):141-158.

Yang, X., R. C. Malak, C. Lauer, C. Weidig, H. Hagen, B. Hamann, J. C. Aurich, and O. Kreylos. 2015. "Manufacturing System Design with Virtual Factory Tools." *International Journal of Computer Integrated Manufacturing* 28(1): 25-40.

AUTHOR BIOGRAPHIES

SANJAY JAIN is an Associate Professor in the Department of Decision Sciences, School of Business at the George Washington University. Before moving to academia, he accumulated over a dozen years of industrial R&D and consulting experience working at Accenture in Reston, VA, USA, Singapore Institute of Manufacturing Technology, Singapore and General Motors North American Operations Technical Center in Warren, MI, USA. He served as an associate editor of the *International Journal of Simulation and Process Modelling* for 2004-2014 and continues to serve as a member of the editorial board of the *International Journal of Industrial Engineering*. His research interests are in application of modeling and simulation of complex scenarios including smart manufacturing systems and project management. His email address is jain@email.gwu.edu.

DAVID LECHEVALIER is a guest associate in NIST's Systems Integration Division of the Engineering Laboratory. He is a PhD student in the laboratory Le2i at the University of Burgundy. His current research topics include advanced analytics and modeling for Smart Manufacturing. He received a computer science Master's degree in Database and Artificial Intelligence from University of Burgundy in 2012. His email address is david.lechevalier@nist.gov.

JUNGYUB WOO is a research associate in the Systems Interoperability Group in NIST's Software and Systems Division of the Information Technology Laboratory. His current research topics include data standard, data assurance, big data infrastructure and data interoperability for Health Care and Smart Manufacturing. He worked at Samsung SDS before working at NIST. He received a PhD degree in industrial and management engineering from POSTECH in 2008. His email address is jungyub.woo@nist.gov.

SEUNG-JUN SHIN is a guest associate in the Life Cycle Engineering Group in NIST's Systems Integration Division of the Engineering Laboratory. His current research topics include advanced analytics, big data infrastructure and STEP-based data interoperability for Smart Manufacturing. He worked at Samsung Electronics and Samsung SDS before working at NIST. He received a PhD degree in industrial and management engineering from POSTECH in 2010. His email address is seungjun.shin@nist.gov.

Jain, Sanjay; Lechevalier, David; Woo, Jungyub; Shin, Seungjun.
"Towards a Virtual Factory Prototype."
Paper presented at the Winter Simulation Conference, Huntington Beach, CA, Dec 6-Dec 9, 2015.

Fabrication of High Value Standard Resistors for ICE-LMVE

Isabel Castro[1], Dean Jarrett[2], Marlin Kraft[2]

[1]Laboratorio Metrológico de Variables Eléctricas – Instituto Costarricense de Electricidad, San Pedro de Montes de Oca, San José, Costa Rica. Tel: +506-2001-2374, email: bcastro@ice.go.cr

[2]National Institute of Standards and Technology, 100 Bureau Drive, Stop 8171, Gaithersburg, MD, 20899, USA. Tel: +301-975-4240, Fax: +301-926-3972, email: dean.jarrett@nist.gov. Tel: +301-975-4239, Fax: +301-926-3972, email: marlin.kraft@nist.gov

***Abstract* — In Costa Rica, the Laboratorio Metrológico de Variables Eléctricas (LMVE) at the Instituto Costarricense de Electricidad (ICE) develops and improves measurement capabilities to promote and support the industrial innovation and development in the country. It's a pertinent remark that the resistance standards as well as the dc voltage standards are used to determine other electrical quantities such as electrical power, energy, electrical current or capacitance. A set of nineteen high value standard resistors from 100 MΩ to 100 GΩ were fabricated and measured at the National Institute of Standards and Technology (NIST). A subset of these standard resistors will be used as resistance standards for ICE-LMVE.**

***Index Terms* — Measurement, resistance standards, measurement techniques, precision, stabilization time, uncertainty.**

I. Introduction

A joint project on high resistance standards was conducted at the National Institute of Standards and Technology (NIST) with a guest researcher from the Instituto Costarricense de Electricidad (ICE) during 2015. The project was in support of the NIST strategic alliances with the institutions participating in the Inter-American System of Metrology (SIM) and NIST commitment to strengthening the measurement infrastructure in the Americas. The ICE guest researcher collaborated in the construction of high resistance standards in the range of 100 MΩ to 100 GΩ as well as scaling and measurement techniques using the dual source bridge method [1]. The results of this collaboration will improve the traceability chain for high resistance measurements used by ICE. Knowledge of other measurement techniques, such as the use of guarded Hamon transfer standards, direct current comparator bridges, and teraohmmeters were also part of the training program at NIST [2].

II. High Value Resistance Standards for Measurement and Calibration

The high resistance standards (up to 100 GΩ) available in the ICE-LMVE to perform their measurement and calibration work are commercial air-type resistance standards. These resistors are used as primary, working, or transportable transfer standards for the calibration of resistance ranges of multi-function calibrators and multimeters.

ICE-LMVE standards had been calibrated by other National Metrology Institutes (NMI) since 2010. The 100 GΩ resistor had been presenting a particular problem with its long stabilization time, as noted by the calibration provider NMI. Figure 1 shows that at least 1000 s is needed between the moment when the voltage is applied and the moment when the first stable measurement is taken.

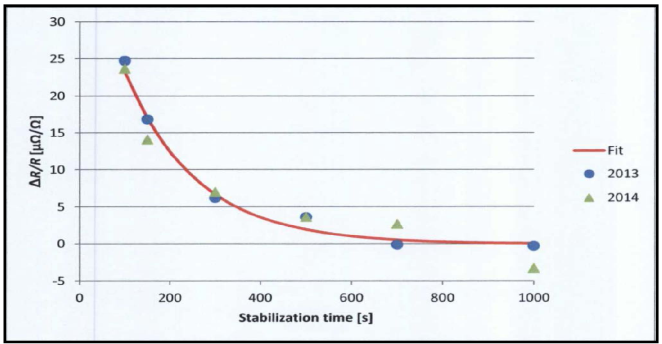


Fig. 1. Example of stabilization time with 1000 V test voltage for the 100 GΩ primary standard resistor used at ICE.

Measurement at ICE of this resistor showed that it has a drift rate of - 50 μΩ/Ω/year, with a temperature coefficient on the order of 250 (μΩ/Ω)/°C and a 1 (μΩ/Ω)/V voltage coefficient. An anticipated outcome of the training program at NIST was to construct a 100 GΩ standard resistor with improved stabilization time, drift, temperature and voltage coefficients for ICE to use as a primary standard in their calibration laboratory.

III. High Value Resistance Fabrication

The main objective in the fabrication of resistances standards was to construct at least one set of high resistance standards (100 MΩ, 1 GΩ, 10 GΩ and 100 GΩ) with good temperature and voltage coefficients, lower stabilization time and low drift with the possibility of a lower difference from the nominal value. The additional set of resistance standards would improve the robustness of the traceability chain and the quality control of high resistance measurements at ICE.

Precious metal-oxide film type resistance elements [3] have good characteristics for tolerance, stability, and temperature coefficient at resistance levels of 1 MΩ and above. Also, the resistors feature low noise and a high linearity because of a

U.S. Government work not protected by U.S. copyright

Jarrett, Dean; Castro, Isabel; Kraft, Marlin.
"Fabrication of High Value Standard Resistors for ICE-LMVE."
Paper presented at the CPEM 2016 Conference, Ottawa, Canada, Jul 10-Jul 15, 2016.

low voltage coefficient and low temperature coefficient, which makes them a good choice for high resistance standards.

The 100 MΩ and 1 GΩ resistance elements were heat treated and then hermetically sealed into cylindrical brass tubes, using glass-to-metal seals soldered to each end of the brass tubes. Near each end of the brass tubes there are also soldered copper tubes used to purge and fill the resistor container with an inert gas to provide a clean and moisture-free environment for the resistor element. Hermetically sealing the resistor element eliminates the seasonal humidity effects of resistance decrease due to surface leakage across the element and stress-induced change due to swelling in insulators in contact with the resistance film. [3]

The 10 GΩ and 100 GΩ resistor elements were hermetically sealed using the same procedures used for the 100 MΩ and 1 GΩ resistor elements except that the solid brass tube was replace with a metal-insulator-metal tube. Polytetrafluoroethylene (PTFE) and borosilicate glass were the insulating materials used. This metal-insulator-metal design allows the metal ends of the tube to be driven at guard potential, suppressing leakage currents flowing across the glass insulator of the seals. [3]

Each hermetically sealed resistance element was packaged in an aluminum enclosure with coaxial connectors as shown in Figure 2. Each terminal of the resistor element was soldered to the inner terminal of an N-type female connector (Glass dielectric type, 50 Ohm Impedance). The outer terminal of each N type connector was soldered to the hermetically sealed container. The N-type connector is mounted on a rectangular PTFE plate on the top panel of an aluminum box, which isolates the N-type connectors from the aluminum box. Each hermetically sealed container uses a support made of visco-elastic material to provide vibration and electrical isolation of the hermetically sealed container from the aluminum box.

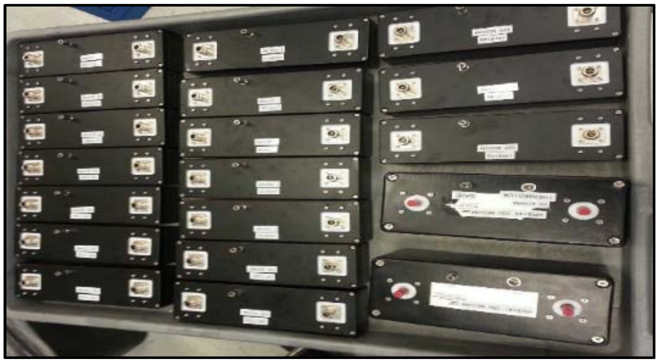


Fig. 2. Final Resistor assembly. 100 MΩ, 1 GΩ, 10 GΩ, and 100 GΩ resistors shown.

VI. Conclusion

A number of measurements were made on the final resistor assemblies in order to check the stabilization time and other characteristics of the resistance standards. Figure 3 shows the stabilization time for one of the 100 GΩ standard resistors fabricated during this project. From 120 s to 300 s, the resistor decreased by approximately 12 μΩ/Ω, but had no discernable change from 300 s to 700 s, indicating that the resistor has a 300 s stabilization time. This is a factor of three reduction from the 1000 s settling time of the 100 GΩ resistor used at ICE. [4]

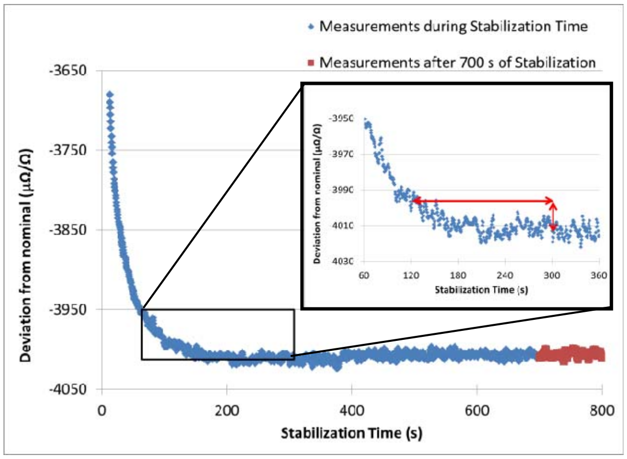


Fig. 3. Example of stabilization time, for a 100 GΩ resistor. Stability achieved after test voltage applied for 300 s.

Due to the natural aging process, the resistance standards long-term drift needs to be monitored in years to come. The expected yearly drift rate for the 100 GΩ resistors is about 10 μΩ/Ω, based on the control charts for similar resistors constructed with resistor elements from the same lot and following the same construction techniques at NIST.

Acknowledgement

I would like to thank NIST and SIM for this six months appointment as a Guest Researcher, and their extraordinary support in this process. I would like to express my gratitude to Dean Jarrett and Marlin Kraft for their expert advice and encouragement throughout this project.

References

[1] L.C.A. Henderson, “A new technique for the automated measure-ment of high valued resistors,” J. Phys. Electron. Sci. Instrum., vol. 20, pp. 492 – 495, 1987.

[2] R. Elmquist, D. Jarrett, G. Jones, M. Kraft, S. Shields and R. Dziuba. “NIST Measurement Service for DC Standard Resistors”, NIST Technical Note 1458, December 2003.

[3] R. Dziuba, D. Jarrett, L. Scott and A. Secula, “Fabrication of high-value standard resistors”, IEEE, vol. 48, no. 2, pp. 333-337, April 1999.

[4] D. Jarrett and R. Elmquist, “Settling times of high-value standard resistors”, CPEM 2004 Digest, p. 522, London, England, Jun, 2004.

“Fabrication of High Value Standard Resistors for ICE-LMVE.”

Quantum Hall Resistance Traceability for the NIST-4 Watt Balance

Dean Jarrett[1], Rand Elmquist[1], Marlin Kraft[1], George Jones[1], Shamith Payagala[2],
Frank Seifert[2], Darine Haddad[2], and Stephan Schlamminger[1]

[1]National Institute of Standards and Technology, 100 Bureau Drive, Stop 8171, Gaithersburg, MD, 20899, USA
Dean.jarrett@nist.gov

[2]University of Maryland, Joint Quantum Institute, College Park, MD, 20742, USA

Abstract — **Scaling from the quantum Hall resistance to 100 Ω standard resistors used by the NIST-4 watt balance involves multiple resistance standards and bridges to provide the lowest possible uncertainty. Described here is the infrastructure and procedures developed to support these measurements at better than 20 x 10^{-9} standard uncertainty levels.**

Index Terms — **quantum Hall resistance, cryogenic current comparator, direct current comparator, standard resistor, watt balance.**

I. Introduction

The multinational effort to replace the last artifact-based SI definition, the kilogram (kg), has had much attention from the international community and extensive efforts by many national metrology institutes (NMI) in the building of watt balances [1] or in the counting of the number of atoms in a kg of pure silicon [2]. Those experiments are well documented and rely on low uncertainty in voltage, resistance, mass, and gravity. Described here is the infrastructure now in place to provide the NIST-4 watt balance with traceability to the quantum Hall resistance [3] at the 100 Ω level.

At the National Institute of Standards and Technology (NIST), the resistance project has been providing ongoing support for the watt balance work for many years. The NIST-3 and earlier watt balances were all situated in a remote building on the NIST campus. An adequate solution for that situation was to carefully transport 100 Ω resistance standards on a periodic basis between the two locations and maintain control charts to track the drift rates and changes in resistance.

As the NIST Advanced Measurement Laboratory (AML) was conceived twenty years ago, having a future watt balance located in close proximity to the quantum standards of resistance and voltage was a design feature. Transporting resistors less than 50 m or calibrating them in-situ within the AML is a better situation than having to transport them 1.5 km from one building to another on the NIST campus. Reducing handling and shorter calibration intervals of the 100 Ω resistors for NIST-4 reduces uncertainty.

II. Traceability from QHR to 100 Ω

The NIST quantum Hall resistance (QHR) has been the national standard for resistance since January 1, 1990 [3]. Typically the system is operated two to three times a year to calibrate and adjust the drift rates of several banks of reference standards. The most direct link to the QHR is a bank of five 100 Ω standard resistors which are calibrated directly against the QHR $i = 2$ plateau of 12 906.4035 Ω during the operation of the QHR. A cryogenic current comparator (CCC), with a turn ratio of 4130:32, has been used to make this transfer for many years [3]. NIST has recently brought into service a binary cryogenic current comparator (BCCC) with multiple turn ratios, up to 2065:16, which can also be used for this first step from the QHR as well as other ratios such as 10:1 [4]. Other 100 Ω resistors, such as those used for NIST-4, may also be calibrated by the CCC or BCCC with the QHR as a standard when the QHR is being operated. Due to the time, labor, and expense of keeping the QHR system cold at 0.3 K, it is not practical to operate year round. During times when the QHR is not being operated, 100 Ω resistors may be calibrated with the 100 Ω reference bank. Resistors in this bank have relative drift rates ranging from 0.025 x 10^{-6} / year to 0.351 x 10^{-6} / year. Calibrations using the 100 Ω reference bank may be done by the CCC, the BCCC, or one of the direct current comparator (DCC) bridges with matrix scanners [5]. All three of these systems provide the lowest Type A uncertainty with a two-step process which calibrates a 10 Ω, 1 kΩ, or 12.9 kΩ standard resistor before calibrating a 100 Ω resistor. Power coefficients need to be taken into consideration if transferring through a 10 Ω resistor at different current levels. The 10:1, 2065:16, or 4130:32 bridge ratios have lower Type A uncertainty than a 1:1 ratio [6].

III. Location of Bridges and Infrastructure

Figure 1 shows that most of these bridges and standard resistors are located in the main resistance laboratory in room F013 of the AML. The QHR is in this lab in an isolated pit. The NIST-4 watt balance is located in the next corridor in room E024, also in an isolated pit. Due to limited space in E024, the 100 Ω resistors are located in a different room via a shielded four-terminal cable (as had been done for NIST-3). The availability of space in room F023, which is adjacent to F013 and directly across the corridor from E024, was an appropriate location. F023 is a shielded laboratory space with less activity than the main resistance laboratory of F013, providing isolation of the 100 Ω resistors and NIST-4 measurements from other activities taking place in the main resistance lab of F013. A DCC and matrix scanner are located in F023 which calibrates the 100 Ω resistors for NIST-4 regularly. Dedicated air and oil baths and check standards are

U.S. Government work not protected by U.S. copyright

Jarrett, Dean; Elmquist, Randolph; Kraft, Marlin; Jones Jr., George;
Payagala, Shamith; Seifert, Frank; Schlamminger, Stephan; El Haddad, Darine.
"Quantum Hall Resistance Traceability for the NIST-4 Watt Balance."
Paper presented at the CPEM 2016 Conference, Ottawa, Canada, Jul 10-Jul 15, 2016.

also in F023. A four-terminal double-shielded junction-box is installed in F023 to allow connection to any of the 100 Ω resistors in F023 to NIST-4, the DCC bridges, the CCC bridge, or the BCCC bridge. A 30 m double-shielded cable goes from NIST-4 in E024 to the junction box in F023. Likewise, two double-shielded cables of length 30 m go from the junction box in F023 to the CCC and BCCC bridges and 100 Ω reference bank in F013. The double-shielded cables and junction box have made it possible to calibrate the 100 Ω resistors used by NIST-4 in-situ without having to move or disturb them for calibration or connection to the experiment, reducing errors due to transportation and handling.

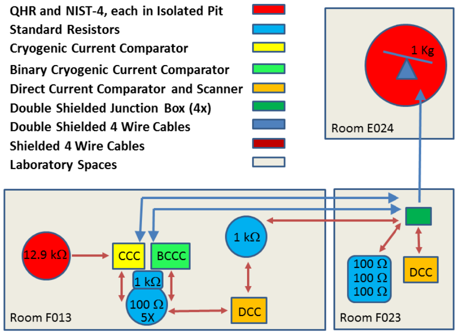

QHR and NIST-4, each in Isolated Pit
Standard Resistors
Cryogenic Current Comparator
Binary Cryogenic Current Comparator
Direct Current Comparator and Scanner
Double Shielded Junction Box (4x)
Double Shielded 4 Wire Cables
Shielded 4 Wire Cables
Laboratory Spaces
1 Kg
Room E024
12.9 kΩ
CCC
BCCC
1 kΩ
1 kΩ
100 Ω
5X
DCC
Room F013
100 Ω
100 Ω
100 Ω
DCC
Room F023

Fig. 1. Location of the QHR, NIST-4, CCC, BCCC, DCCs, resistors, double-shielded junction box, and 4 wire cables. Multiple paths are shown to scale from the QHR to resistors used by NIST-4.

IV. Measurement Results

The infrastructure described has been in place and refined since 2015. Routine measurement of the 100 Ω resistors, located in F023, has been done by a DCC located there to calibrate and track the drift of the resistors. The automated switching of the matrix scanner has made weekly measurement of these resistors and check standards possible. Less frequently, the 100 Ω resistors have been calibrated using the CCC and BCCC and 100 Ω reference bank in F013. Resistors must be manually connected to the CCC or BCCC so these processes are more labor intensive than using the DCC and matrix scanner. A comparison of the DCC and BCCC to calibrate the 100 Ω resistors in F023 yielded agreement of 3 x 10^{-9} for these systems, using resistors in the 100 Ω reference bank in F013 as the standards. We have recently been successful at remote calibration of the 100 Ω resistors in F023, through the double-shielded cable, using the QHR standard and the CCC and BCCC bridges. Additional measurements are planned when the QHR is operated in 2016.

Figure 2 shows a recent test using both lengths of the 30 m double-shielded cables connected in series (60 m) with the DCC and 100 Ω reference bank in F013, without moving resistors. The 100 Ω measurements made with and without the 60 m cable agreed within 4 x 10^{-9} for the DCC and BCCC. Initial measurements were 10 x 10^{-9} from the predicted value of the 100 Ω. Updating the calibration of the 10 Ω and 1 kΩ reference resistors brought the 100 Ω measurements within 5 x 10^{-9} of the predicted value. Changes in barometric pressure have been correlated to the post-calibration change in the measurements made using the 1 kΩ standard.

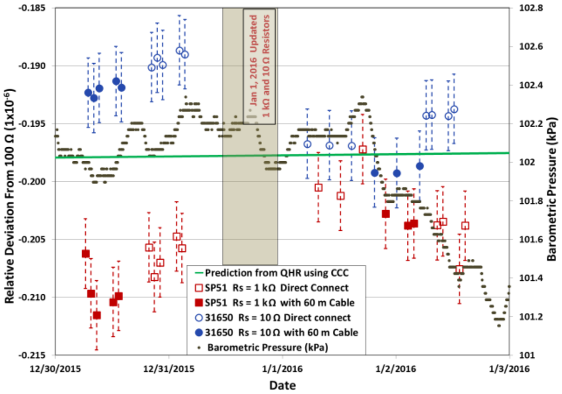


Fig. 2. Test of double-shielded cables without moving the standard resistors. 100 Ω resistors in F013 were measured by the DCC and BCCC with a direct connection and with 60 m of double-shielded cable from F013 to F023 and back to F013 inserted agreed within 4 x 10^{-9}. Only DCC measurements are shown. Error bars are typical 1σ standard deviation of the measurements.

V. Conclusion

The system of bridges, standard resistors, and connections for providing traceability from the NIST QHR to the NIST-4 watt balance is described. The system provides in-situ calibration of the 100 Ω standard resistors used by NIST-4. A comparison of the BCCC and DCC bridges agreed within 3 x 10^{-9}. Recent tests of the double-shielded cables with the DCC and BCCC demonstrated a difference of less than 4 x 10^{-9} for measurements made with and without the 60 m of double-shielded cable. Frequent calibration of 10 Ω and 1 kΩ reference resistors is critical for measurements to agree within 5 x 10^{-9}. Additional tests of the scaling from the QHR to the 100 Ω standard resistors for NIST-4 are ongoing.

References

[1] "Watt and joule balances, the Planck constant and the kilogram," *Metrologia*, 51 (2), S1 - S140, 2014.

[2] "International determination of the Avogadro constant," *Metrologia*, 48 (2), S1 - S120, 2011.

[3] F. Delahaye, T. J. Witt, R. E. Elmquist, and R. F. Dziuba, "Comparison of the quantum Hall effect resistance standards of the NIST and the BIPM," *Metrologia*, 37, 173-176, 2000.

[4] D. Drung, M. Gotz, E. Pesel, H. J. Barthelmess, and C. Hinnrichs, "Aspects of Application and Calibration of a Binary Compensation Unit for Cryogenic Current Comparator Setups," *IEEE Trans. Instrum. Meas.*, v. 62, n. 10. pp.2820-2827, 2013.

[5] R. Elmquist, D. Jarrett, G. Jones, M. Kraft, S. Shields and R. Dziuba. "NIST Measurement Service for DC Standard Resistors", NIST Technical Note 1458, December 2003.

[6] N. Kaneko, T. Oe, W. S. Kim, D. H. Chae, R. Elmquist, and M. Kraft, "Transportation Effects and Basic Characteristics of Metal-Foil Resistors Examined in an International Trilateral Pilot Study," *IEEE Trans. Instrum. Meas.*, vol. 64, no. 6, pp. 1514-1519, 2015.

"Quantum Hall Resistance Traceability for the NIST-4 Watt Balance."

Third Generation of Adapted Wheatstone Bridge for High Resistance Measurements at NIST

Dean G. Jarrett[1], Shamith U. Payagala[2], Marlin E. Kraft[1], and Kwang Min Yu[3]

[1]National Institute of Standards and Technology, 100 Bureau Drive, Stop 8171, Gaithersburg, MD, 20899, USA
Dean.jarrett@nist.gov

[2]University of Maryland, Joint Quantum Institute, College Park, MD, 20742, USA

[3]Korean Research Institute of Standards and Science, P.O. Box 102, Yusong, Daejon, 305-600, Korea

***Abstract* — A third generation of adapted Wheatstone bridge is being developed at the National Institute of Standards and Technology (NIST) to improve high resistance measurements and scaling from 1 TΩ to 10 PΩ. Improvements to extend range and reduce uncertainties include: automated calibration of the voltage sources, modified bridge balancing algorithm, low-noise shielded cables, and software migration to a modern programming environment. Initial measurements agree well within the expanded uncertainties (k = 2) of the second generation NIST adapted Wheatstone bridge.**

***Index Terms* — standard resistor, high resistance, voltage source, calibration, adapted Wheatstone bridge.**

I. INTRODUCTION

The adapted Wheatstone bridge [1] is an automated measurement technique for the measurement of high resistance standards in the range 10 MΩ to 100 TΩ. An adapted Wheatstone bridge uses low-impedance programmable dc sources (V_1, V_2) in place of two of the resistive ratio arms of a conventional Wheatstone bridge. High resistance standards (≥ 1 MΩ) (R_X, R_S) are used in the other two ratio arms. When the bridge is balanced, the unknown resistor value (R_X) can be determined as

$$R_X = R_S\,(V_1/V_2). \qquad (1)$$

The technique has been used at the National Institute of Standards and Technology (NIST) [2] as well as at other national metrology institutes for measurement of high resistance standards to at least 100 TΩ [3]. The first and second generation adapted Wheatstone bridges at NIST have been in service since 1996 and 2008, respectively. These systems continue to be extensively used for high resistance measurement services and research work at NIST. The age of the software platform, desired modification of the balancing algorithm for measurements above 1 TΩ, and improvements to the voltage source calibration are several factors that made the development of a third generation adapted Wheatstone bridge appropriate at this time.

The earlier NIST adapted Wheatstone bridges use guarded Hamon transfer standards and the substitution technique to build up from lower resistance values in decade steps [4]. Most Hamon transfer standards have ten resistors of the same nominal value which are permanently connected in series. Paralleling fixtures are used to connect the resistors in parallel or series-parallel configurations allowing 1:100 and 1:10 ratios for scaling to higher resistance levels. The guard circuit [2] maintains approximately the same potential as the main circuit at each junction, thus suppressing leakage currents to ground.

The availability of guarded Hamon transfer standards has made the scaling process less dependent on the uncertainty contribution of the voltage ratio as any systematic offsets in voltage at a given range tend to cancel when standard resistors of the same nominal value are measured by the substitution method. For measurements above 1 TΩ, direct calibration of the voltage sources to better than manufacturer specification (6 μV/V) is necessary for evaluating the guarded Hamon transfer standards where parallel to series (1:100) and series-parallel to series (1:10) transfers have been difficult to verify.

The measurement of Wye-Delta resistance networks [5] is difficult with the existing balancing algorithm which drives the bridge to ± 5000 x 10^{-6} from null and extrapolates the bridge null from a linear fit. Accurate measurement of a Wye-Delta network requires the low terminal to be at the same potential as the case or ground (i.e. bridge null condition), which is not the situation for the first and second generation NIST adapted Wheatstone bridges.

II. CHANGES TO THE THIRD GENERATION BRIDGE

Over the years, there were improvements to the first and second generation bridges, such as ramping of voltage sources and addition of coaxial automated switching, but no major changes were made to the measurement sequence or balancing algorithm. The dated programming environment along with the eclectic nature of the code made it sensible to make significant changes to the software in a modern programming environment that is widely supported and less likely to be obsolete in the future.

A. Voltage Source Calibration

An interchange of the voltage sources in the third generation bridge yielded a difference in R_X of 6 μΩ/Ω for a 1:1 bridge ratio. Two methods were tested to improve the voltage ratios and reduce this interchange difference to less than 1 μΩ/Ω. The first method was to use a calibrated digital volt meter (DVM) to measure the output of each voltage source and use those voltage measurements in the calculation of the unknown resistance. The second method was to

U.S. Government work not protected by U.S. copyright

Jarrett, Dean; Payagala, Shamith; Kraft, Marlin; Yu, Kwang Min.
"Third Generation of Adapted Wheatstone Bridge for High Resistance Measurements at NIST."
Paper presented at the CPEM 2016 Conference, Ottawa, Canada, Jul 10-Jul 15, 2016.

calibrate the voltage sources against Zener voltage references with an automatic potentiometer and 1200 V range extender at all voltage ranges and store those corrections in tables for recall during the resistance measurement. While both methods reduced the interchange offset error, the second method was selected due to ease of calibration of the voltage sources with the automatic potentiometer, shorter resistor measurement time by not adding voltage measurements to the process, and avoidance of possible issues with switching or ranging of the DVM.

B. Balancing Algorithm and Null Current Measurement

The third generation bridge balances to a true null rather than ± 5000 x 10^{-6} from null as in the earlier NIST bridges. To minimize the effects of detector and bridge offsets, the measurement sequence starts with measuring the bridge null current (I_{null}) when $V_1 = V_2 = 0$. A pre-balance is done next where V_1 is set to the test voltage of R_X and V_2 is set so V_1/V_2 is the same nominal ratio as R_X/R_S and the detector current (I_D) is measured. The null and detector current measurements are used in equation 2 to determine V_2' for the bridge null balance as

$$V_2' = V_2 + (I_D - I_{null})R_S. \qquad (2)$$

With the voltage sources set to V_1 and V_2', the detector current I_D' is now measured with the bridge balanced. The bridge is balance if the difference of I_D' and I_{null} is less than the detector resolution for the current range. If this condition is not met, an additional adjustment of V_2 is performed and the current measurement repeated. After all iterations, the bridge null current measurement, where $V_1 = V_2 = 0$, is repeated to verify that there is no significant drift in the bridge during the measurement sequence. The process is then repeated for the reverse polarities of V_1 and V_2. Once the measurement sequence is completed, corrections for V_1, V_2, and R_S are applied and R_X is calculated from equation 1. Measurements are typically made 120 s to 300 s (3600 s maximum) after voltage is applied to allow the RC time constants of the system to dissipate. V_1 and V_2 are of opposite polarity.

III. DATA AND RESULTS

The third generation bridge uses the calibrated voltage ratio V_1/V_2 and the standard resistor R_S to determine R_X which is different from the second generation bridge which relies on the substitution technique and guarded Hamon transfer standards. Measurements at 10 TΩ showed the two methods to agree within 50 μΩ/Ω, which is quite acceptable considering possible transfer errors of the guarded Hamon transfer standard at this resistance level. Further testing with an additional Hamon transfer standard at 1 TΩ is planned.

Measurements were also made at 1 PΩ and 10 PΩ using Wye-Delta networks configured from NIST standards and compared to a potentiometric measurement technique [6]. Figure 1 shows measurements made with the third generation bridge and the potentiometric method on a Wye-Delta network assembled from well characterized high resistance standards at 1 PΩ. Similar results were obtained on two other Wye-Delta networks at 1 PΩ and one at 10 PΩ.

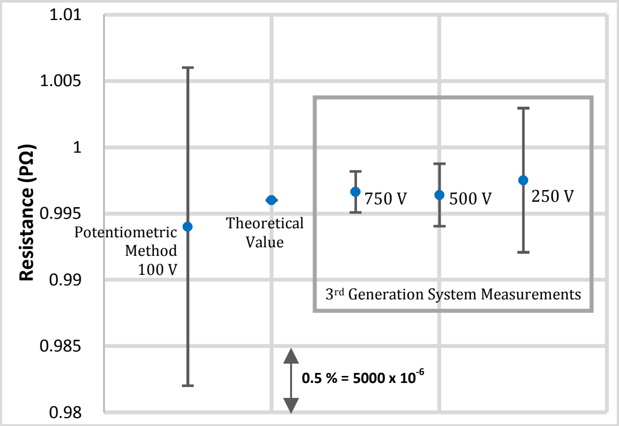


Fig. 1. Measurements made on Wye-Delta networks at 1 PΩ. Error bars are the 1σ standard deviation of multiple measurements over several days. Third generation NIST bridge measurements at several voltages are shown in box to the right. Measurements made on the same Wye-Delta network using the potentiometric method and the theoretical values are shown to the left.

IV. CONCLUSION

The third generation of adapted Wheatstone bridge for high resistance measurements at NIST was built. Improvements include automation of the voltage source calibration and changes to the balancing algorithm which have allowed measurement of Wye-Delta networks. These are shown to result in improved scaling from 1 TΩ to 100 TΩ, which was dependent on guarded Hamon transfer standards. Range has been extended by two orders of magnitude to 1 PΩ and 10 PΩ. These improvements will allow reduction of measurement uncertainties in the 1 TΩ to 100 TΩ range by a factor of three to five.

REFERENCES

[1] L. C. A. Henderson, “A new technique for the automated measurement of high valued resistors,” J. Phys. Electron. Sci. Instrum., vol. 20, pp. 492 – 495, 1987.

[2] D. G. Jarrett, “Automated guarded bridge for calibration of multi-megohm standard resistors from 10 MΩ to 1 TΩ,” IEEE Trans. Instrum. Meas., vol. 46, no. 2, pp. 325-328, April 1997.

[3] G. Rietveld and J.H.N. van der Beek, “Automated High-Ohmic Resistance Bridge with Voltage and Current Null Detection”, IEEE Trans. Instrum. Meas., vol. 62, no. 6, pp. 1760-1765, 2013.

[4] R. Elmquist, D. Jarrett, G. Jones, M. Kraft, S. Shields and R. Dziuba. “NIST Measurement Service for DC Standard Resistors”, NIST Technical Note 1458, December 2003.

[5] H. A. Sauer, “Wye-Delta Transfer Standards for Calibration of Wide Range dc Resistance and dc Conductance Bridges,” IEEE Trans. Instrum. Meas., vol. 17, no. 2, pp. 151-155, June 1968.

[6] K. M. Yu, W. S. Kim, S. H. Lee, K. S. Han, J. H. Kong, “A method for measuring high resistances with negligible leakage effect using one voltage source and one voltmeter,” Meas. Sci. Technol., 25, 2014.

“Third Generation of Adapted Wheatstone Bridge for High Resistance Measurements at NIST.”

Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 57 (2016) 686 – 691

www.elsevier.com/locate/procedia

49th CIRP Conference on Manufacturing Systems (CIRP-CMS 2016)

Understanding sustainability data through unit manufacturing process representations: a case study on stone production

Laurie Rebouillat[a]*, Ilaria Barletta[a], Björn Johansson[a], Mahesh Mani[bc], William Z Bernstein[c], KC Morris[c], Kevin W Lyons[c]

[a]Chalmers University of Technology, Product and Production Development, 41296 Göteborg, Sweden
[b]Dakota Consulting Inc., 20910 Silver Spring, MD, USA
[c]National Institute of Standards and Technology, 20899 Gaithersburg, MD, USA

* Corresponding author. Tel.: +4631-7721000; fax: +4631-7223660. *E-mail address:* laurie.rebouillat@ifma.fr

Abstract

Efficiency of natural stone production processes in quarries directly affects the economic output and environmental performances, such as production lead times and energy consumptions. Knowledge on stone production processes is crucial in making responsible decisions in this business. Having a structured representation of information characterizing the stone production processes will support stakeholders in better assessing production resources in terms of sustainability and productivity. Value stream mapping can provide an overview and guidance for sustainability performance evaluation, but its application is limited. The challenges arise when trying to specifically map and relate sustainability data between processes e.g., variability in lead time and CO_2 emissions. Manufacturing process characterization standards currently being developed by ASTM International manifest the potential to not only fill this gap but also to provide opportunities to characterize and compose manufacturing processes with relevant environmental information and description. This paper shows the application and lessons learned from deploying one such effort towards standardization.

© 2016 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the scientific committee of the 49th CIRP Conference on Manufacturing Systems

Keywords: Sustainable Production; Natural Stone Production; Unit Manufacturing Process; Composability; Quarrying; Standardization.

1. Introduction

Sustainability, representing a triple-bottom line [1], has become a driver for competitiveness in practically all industrial sectors today. This study focuses on evaluating the sustainability aspects using standard process representations applied on the quarrying processes within natural stone production. The available production technology today demands the use of non-renewable resources, thus causing several negative impacts on the environment. Examples are air pollution from dust and CO_2 emissions from the energy utilized for the quarrying machinery in e.g. the cutting processes [2]. These negative impacts drive the companies operating in this sector to improve sustainability performances of quarrying processes.

Understanding the business processes modelling of an organisation is preliminary for determining its success [3]. Business process was earlier defined as "the combination of a set of activities within an enterprise with a structure describing their logical order and dependence whose objective is to produce a desired result" [3]. This is apt for the natural stone production. The business processes of interest are actual manufacturing processes, which include processes of stone production occurring within quarries.

Understanding the natural stone production process can be rather involved. Several different factors within the production processes vary in quality and performance, and hence the overall output has a large variability as well. Representative factors include:

2212-8271 © 2016 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the scientific committee of the 49th CIRP Conference on Manufacturing Systems
doi:10.1016/j.procir.2016.11.119

- Natural factors: e.g., adverse atmospheric conditions, natural tension in the rock, colour variations of the stones
- Location of cracks in the stones
- Different manufacturing processes that can be used for the stone forming phases e.g., drilling, blasting, wire sawing, and wedging.
- Weather related uncertainties

With such uncertainties, a structured understanding of processes for natural stone production would further provide a basis for improvement with respect to sustainability performance. From a sustainability point of view, successful stone production within quarries means producing larger volumes with higher output quality, while at the same time, reducing the risk of injury and environmental influences. Sustainability data describing manufacturing processes related to economic (operational) and environmental sustainability will be the focus of this study. This coincides with the goals of the VINNOVA-funded project on “Efficient and sustainable natural stone production” [4], in the context of this research.

We hypothesize that a structured, sustainability-oriented representation of individual manufacturing processes will provide a strong baseline for engineers and managers to meticulously understand and improve sustainability performances of the natural stone production. This paper aims at testing such a hypothesis by implementing a new representation designed for unit manufacturing processes based on an ASTM International [14] standards effort.

The paper is organized as follows: Section 2 reports on the state of art methodologies to map process information within quarrying and mining, Section 3 describes the standard representation used in this study, Section 4 illustrates the application of the standard on a quarry. Section 5 presents a discussion on the practicality and limitations of the standard for the natural stone production industry. Moreover, it shows the standard’s future developments.

2. State-of-art on mining and aggregates

Because of the inherent complexity of natural stone production, it follows that a standard aiming at representing quarrying process data under the sustainability lens must be both beneficial to model operational and environmental data. Different methods for process modelling have been used within manufacturing systems [3][5]. In order to specifically investigate the use of process modelling applied to aggregates and mining, the authors performed a literature review within Scopus, Web of Science and Google Scholar databases. From the review, the following conclusions were made:

- the use of simulation models in quarrying exists [6-8], specifically for production-related performances
- various process modelling tools have been applied to model mining and quarrying processes, like for instance Petri nets [9] and value stream mapping (VSM) [10]
- no specific reports addressing the process data in quarrying from a sustainability perspective.

As a result, the authors aim at mapping manufacturing processes of quarries by utilizing standardized representations which supports both operational and environmental data modelling.

3. Standard representations for manufacturing processes

To effectively compute sustainability performance of manufacturing processes and to facilitate decision making, sustainability-related standards are currently being developed by ASTM International [11]. There is a transformation of manufacturing industries from environmental practices based on human experience to environmental practices based on science, specifically on science-based sustainability characterization [12, 13]. That transformation is captured in the Guide for Characterizing Environmental Aspects of Manufacturing Processes [14]. The guide outlines a characterization methodology and proposes a generic representation from which manufacturers can derive specific unit manufacturing process (UMP) representations for meaningful sustainability performance analysis, see Fig. 1.

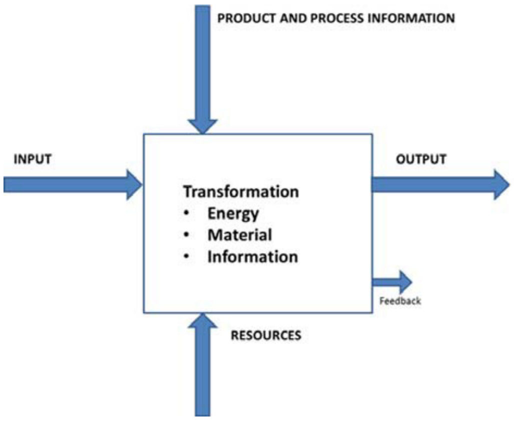


Fig. 1. Graphical representation of a UMP.

Graphical and programming methods can be used to build the UMPs. The creation of a network of UMPs can then be made using the graphical method and transcribed in the formal method (for example in XML).

According to the guide [14], sustainability characterization involves:

1) Identifying the UMPs including key performance indicators and the specifying boundaries,
2) Identifying UMP specific attributes that includes the specific inputs, manufacturing resources, product and process information, and outputs for each UMP,
3) Identifying the transformation functions and listing key UMP specific variables required for calculating the transformation equations.

Inputs include material and consumables; product and process information includes process specifications, production plan, equipment specifications, material specifications, etc.; resources include equipment/tooling, software, etc.; and outputs include product, by-product and waste. Transformation may include material transformation (e.g. mass change, phase change, structure change, deformation, and consolidation), energy transformation (e.g. include chemical, electrical, thermal, mechanical, and electromagnetic) or information transformation such as production metrics (e.g. throughput and overall equipment effectiveness) and environmental metrics (e.g. energy, material, water, emissions, and waste).

The standard purports that in order to realize the utility of the UMPs it is expected that most manufacturers will look towards linking a number of UMP's together to characterize specific production plans for a part, assembly, or a product. This will enable manufacturers to extend the measurement of sustainable performance beyond the process to the product itself. The standard was used as concept guide to model the stone production in three quarries. One of these quarries is used as an example case.

4. Case study

4.1. Overview of Natural Stone Production Processes

In this case study we consider a quarry of grey granite production, where the ideal final products are 2 m^3 stone blocks. In practice, only about 20% of the total production results in the desired final two cubic meters square stone blocks with low variability. The other stone blocks are subsequently classified according to their final shape, their variability. It can be challenging to consider the environmental requirements in this quarry to do any major improvements to production and cost efficiency by acting directly on the process.

The production of one block could consists of four steps. The first step consists of cutting a primary block in the quarry. In the quarry being studied, the use of a wire saw is impossible because of the natural tension in the rock. The process used today to make a primary block is drilling and blasting the drilled holes with explosives (top part of Fig. 2). Once the primary block is made, the second step is to drill and blast the primary block into several smaller secondary blocks.

This second step (middle part of Fig. 2) consists of drilling and wedging specific areas of the block in order to avoid small cracks and discolouring of the stone. This is to create as high quality products as possible.

Secondary blocks are reworked in a third step according to their variability and their shape with a wire saw and drilling/wedging, making the two cubic meter stone blocks from the product, as shown in the lower part of Fig. 2.

The fourth step is to drill and cut the underside of the primary block to make it free.

The location of the final block storage is analysed as one criteria in order to minimize the overall fuel consumption occurring from the inbound logistics, which affects the overall efficiency as well as the environmental impact from the stone production at the quarry.

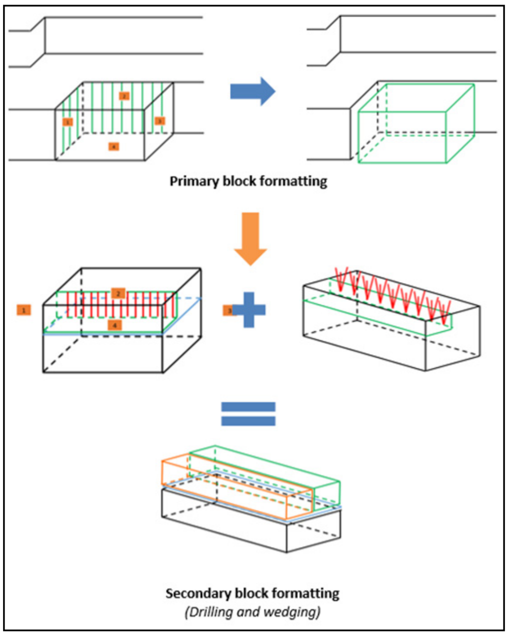


Fig. 2. Illustration of Primary block formatting (drilling and blasting) process

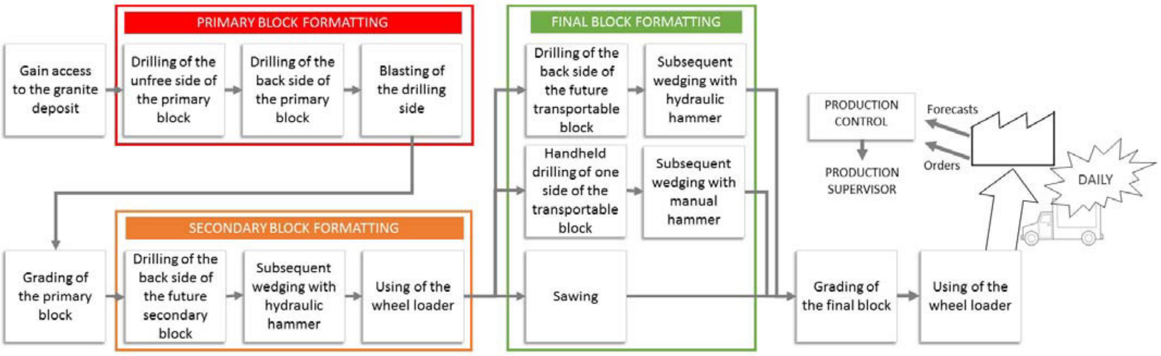

PRIMARY BLOCK FORMATTING
Gain access to the granite deposit
Drilling of the unfree side of the primary block
Drilling of the back side of the primary block
Blasting of the drilling side
FINAL BLOCK FORMATTING
Drilling of the back side of the future transportable block
Subsequent wedging with hydraulic hammer
Handheld drilling of one side of the transportable block
Subsequent wedging with manual hammer
PRODUCTION CONTROL
PRODUCTION SUPERVISOR
Forecasts
Orders
DAILY
SECONDARY BLOCK FORMATTING
Grading of the primary block
Drilling of the back side of the future secondary block
Subsequent wedging with hydraulic hammer
Using of the wheel loader
Sawing
Grading of the final block
Using of the wheel loader

Fig. 3. VSM of the value adding UMPs

4.2. Implementation of the standard

The implementation of the standard on this quarry began by first identifying the different UMPs. In order to identify individual UMPs, it is necessary to understand all the different steps of the production process. To achieve this knowledge, interviews and site visits were conducted to gather the required UMP information from all three quarries. 15 UMPs were identified in the quarries. The flow of the VSM of the 15 UMPs is presented in Fig. 3.

The attributes for each UMP comprising the whole quarrying process is first defined individually. This includes information such as supply and demand of fuel, time, electricity, water, as well as CO_2 emissions. Then by properly creating the connections among individual UMPs, the complete system of the quarry is composed as shown in Fig. 4.

According to the XML syntax, available through the standard guide, it is possible to link attributes of the same type. As inputs and outputs of each UMP; material, energy, wastes and indicators can be considered.

Feedbacks can also be included as outputs of a UMP, for example to calculate the consumption of the resources used by the UMPs. The identified process parameters of each UMP were for example drilling speed, water consumption rate, fuel consumption per meter travelled etc. Those process parameters are then used in the transformation functions inside each UMP to calculate the input/output relationship.

When all UMPs are specified in the formal XML structure, it is possible to compose a network of UMPs by linking outputs and inputs from the different UMPs, as long as they have the same type of data (e.g., “water”, “CO_2”, “stone”). The creation of the linking variables was in this case done within a prototype software demonstrator created to visualize the composed models of the standard.

This demonstration software can also export an automatically transcribed XML file describing each UMP as well as their relation in compliance with the standard.

4.3. Demonstration software

Finally, the ability to compose UMPs was validated through demonstration software. See Fig. 4 for a screenshot of the network of UMPs, which also can be represented in the XML schema for the ASTM standard.

For this case study, the standard is used for modelling the production of stone blocks with UMPs such as “P3_Blasting” and “P4_Grading” as shown in Fig. 4. The production of stone blocks in the quarries are also linked to, for example, water consumption, fuel consumption and CO_2 emissions. Note that, it is also possible to compose models with the standard that take into account data such as fuel quantity necessary to drive a certain distance to, from, and inside the quarry.

The new guide provides the necessary structure and procedure for identifying and capturing key information needs to assess manufacturing performance. By linking individual UMP models together we can create a network or system of UMP models to represent a production system. The demonstrator built on the standard supports a plug-and-play approach to represent the actual flow of material, energy, and information between manufacturing systems for different levels of automation.

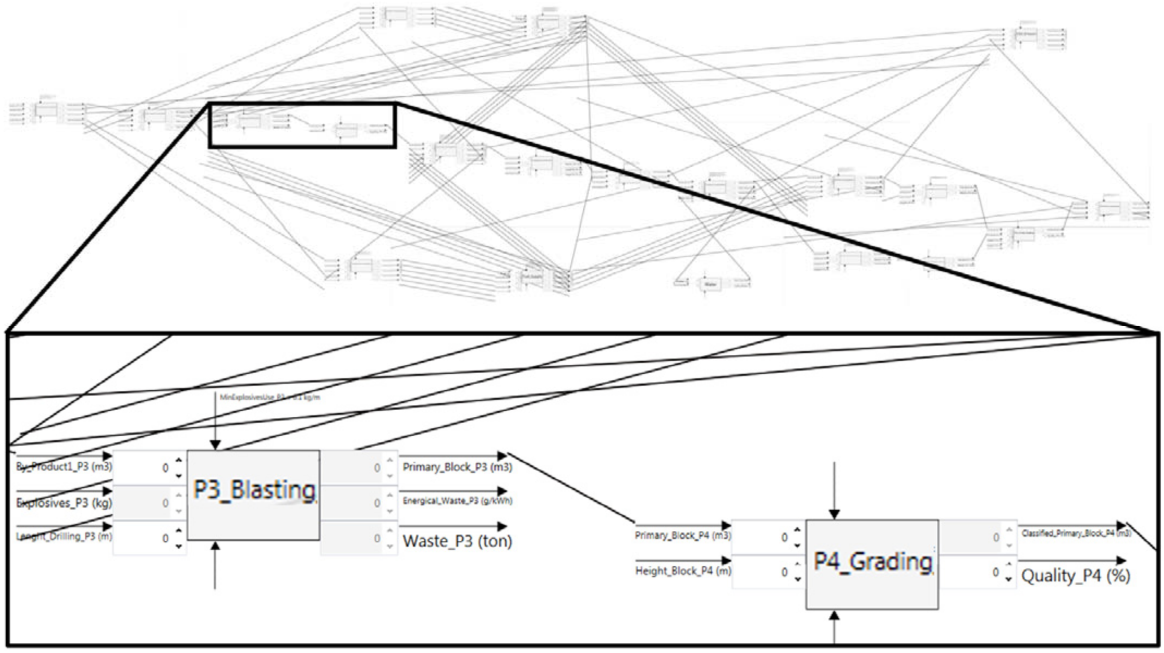


Fig. 4. Example of a network of UMPs

5. Discussion

Standard representations per ASTM E3012-16 [14] provided a baseline for decision makers to holistically understand the natural stone production. UMP representations of individual quarrying processes specifically expanded our understanding of the process performances by tracking the productivity and sustainability related data. Linking multiple UMPs provided the opportunities to build a comprehensive production system enabling analysis and decision support in terms of productivity and environmental.

Collecting the UMP specific information was a crucial part of the study and was done through interviews and site visits. Though initially time consuming, this step was the foundation for the subsequent analysis.

In terms of practicality, the standard was easy to comprehend and use. As was stated in the standard guide, the standard can be used as the backbone while developing modelling tools. In this study, a simple XML based software demonstrator tool was developed. Understanding and implementing the standard using a modelling language such as XML is a learning process.

Besides describing a process, as is possible with tools like VSM, the UMP approach additionally provided opportunities to integrate sustainability and productivity data. It was also easy to account for different types of flows in the same model. VSM is largely used for process mapping, and plots only the time being spent in different processes. It does not factor in the influence of external environmental constraints that is of interest in this study. Hence, the use of VSM is limited whilst studying the quarrying processes under a sustainability perspective.

Some reflections arose from the implementation of the standard through the software demonstrator. During the initial implementation, we noticed that network size of connected UMPs does challenge the implementation of linking variables to read the aggregate data. We are yet to explore the possibility to choose the level of detail (for example, grouping individuals UMPs into one consolidated UMP). There are also opportunities to test different scenarios (i.e., same inputs and outputs but different scenarios for the equations of transformation.)

6. Conclusion and Future Directions

The purpose of this paper is to explore the application of a related ASTM International standard and present lessons learned from its implementation. As described above, the ASTM standard proposes a generic representation from which manufacturers can derive specific UMP representations. These representations are considered as key to achieve meaningful sustainability performance analysis.

To demonstrate the standard's utility, we considered a case study related to natural stone production, since its sub-processes are influenced by high variability, and therefore a structured knowledge representation aids in the business decision making process. Within the case study, we implemented the ASTM standard in order to guide the relative understanding of the sustainability and productivity aspects, both at a unit process level and at a holistic production system level. Preliminary implementation through a simple software demonstrator tool, showed that the standard seems to be easily applicable, adaptable, and helpful for decision support.

Future directions of the work includes (1) improving the prototype tool for the purpose of generalizing its capability to become relevant to any unit manufacturing process, (2) validating its features and general functionality through a formal user evaluation study, and (3) the further development of the prototype tool via a web-based interface, so that other researchers can use its architecture for their own analyses.

A more generalized prototype tool would demonstrate the methodologies robustness to several kinds of analyses, including traditional performance criteria as well as sustainability considerations. From a broader perspective, this work provides insight into the identification of requirements for the implementation of the ASTM standard and its supporting tools. If the standard gains wider adoption, these lessons learned will be critical for moving towards a sharable, distributed manufacturing network, composing of multiple organizations and their suppliers.

Acknowledgements

The authors would like to acknowledge the support from Gauti Asbjörnsson for aiding the cause to conduct the case studies and promoting the work for this paper.

This work was funded by VINNOVA (Swedish Agency for Innovation Systems) through the project “Effektiv och uthållig naturstensproduktion”. This work has been carried out within the Sustainable Production Initiative and the Production Area of Advance at Chalmers. The support is gratefully acknowledged.

Disclaimer

No approval or endorsement of any commercial product, services, or company by NIST is intended or implied.

References

[1] Slaper TF, Hall TJ. The triple bottom line: what is it and how does it work? Indiana Bus Rev. 2011;86(1):4-8.

[2] Abu Hanieh A, AbdElall S, Hasan A. Sustainable development of stone and marble sector in Palestine. J Cleaner Prod. 2014;84:581-8.

[3] Aguilar-Savén RS. Business process modelling: Review and framework. Int J Prod Econ. 2004;90(2):129-49.

[4] VINNOVA. Effektiv och uthållig naturstensproduktion 2014 [cited 2015 Dec 16] Available from: http://www.vinnova.se/sv/Resultat/Projekt/Effekta/2013-04999/Effektiv-och-uthallig-naturstensproduktion/.

[5] Perši N. Conceptual Modelling of Complex Production Systems. J Inf Organ Sci. 2008;32(2):115-22.

[6] Asbjörnsson G, Hulthén E, Evertsson CM. Modelling & Simulation of Dynamic Crushing Plant Behaviour with MATLAB-Simulink. Miner Eng. 2013;43-44(SI):112-20.

[7] Asbjörnsson G, Bengtsson M, Hulthén E, Evertsson CM. Modelling of Discrete Downtime in Continuous Crushing Operation. Computational Modelling 2015, MEI conference 2015.

[8] da Cunha ER, de Carvalho RM, Tavares LM. Simulation of solids flow and energy transfer in a vertical shaft impact crusher using DEM. Miner Eng. 2013;43–44:85-90.

[9] Cordova FM, Canete L, Quezada LE, Yanine F. An Intelligent Supervising System for the Operation of an Underground Mine. Int J Comput Commun Control. 2008;3(3):259-69.

[10] Rylander D. Productivity improvements in construction site operations through lean thinking and wireless real-time control. Västerås: Mälardalen University; 2014.

[11] Subcommittee E60.13 on Sustainable Manufacturing. 2014. http://www.astm.org/COMMIT/SUBCOMMIT/E6013.htm

[12] Mani M, Madan J, Lee JH, Lyons, K.W., Gupta S. Sustainability characterisation for manufacturing processes. Int J Prod Res. 2014:1-18.

[13] Mani M, Madan J, Lee JH, Lyons K, Gupta S. Characterizing sustainability for manufacturing performance assessment. American Society of Mechanical Engineers. 2012:1153–62.

[14] E3012-16 Standard Guide for Characterizing Environmental Aspects of Manufacturing Processes. http://www.astm.org/COMMIT/SUBCOMMIT/E6013.htm

Modeling and Measuring Chloride Ingress into Cracked Mortar

Scott Z. Jones*[1], Jeffrey M. Davis[2], John L. Molloy[3], John R. Sieber[3], Dale P. Bentz[1]

[1] National Institute of Standards and Technology, Materials and Structural Systems Division, US
(E-mail: scott.jones@nist.gov; dale.bentz@nist.gov)

[2] PNDetector GmbH, DE
(E-mail: jeff.davis@pndetector.de)

[3] National Institute of Standards and Technology, Chemical Sciences Division, US
(Email: john.molloy@nist.gov; john.sieber@nist.gov)

ABSTRACT

Chloride ingress into reinforced concrete structures is a cause of corrosion of steel embedded into concrete. To aid in the prediction of concrete service life, a chloride ingress model that includes the effects of physical absorption to and chemical reaction with the cement matrix as well as time-dependent diffusivity is derived by a mass balance and solved by the finite element method. This model is validated through an experimental program where the chloride concentration around cracked specimens is measured using microbeam X-ray fluorescence spectrometry (µXRF). Reinforced mortar beams are cast and cracked by three-point bending. The samples are submerged in a chloride solution for time periods between 7 d and 21 d. The data collected from the µXRF scans is processed using a support vector machine (SVM) algorithm to identify the cement paste matrix. The chloride counts in the matrix are processed by a generalized additive model (GAM) to interpolate the counts over the scan domain. The data is calibrated using standards with known chloride concentrations and the results are compared to the finite element based model which shows good agreement between experiments and modeling. This demonstrates the necessity and usefulness of developing a chloride ingress model that accounts for both chloride ion and cement matrix interactions, the time-dependent behavior of the apparent diffusivity, and crack geometry.

INTRODUCTION

Service life prediction models vary in complexity, from the use of empirical relations for time dependent diffusivity in Fick's Second Law (Vu et al., 2013) to models that capture the effects of water absorption, relative humidity within the pore structure, and ion to ion interactions (Samson et al., 2005). These models do not capture the effects of a crack that may be present in the structure's concrete. The presence of a crack has been shown to dramatically increase the local chloride concentration, at a given cover depth, by providing a preferential pathway for chloride ions to move into the concrete matrix (Bentz et al., 2013, Şahmaran and Yaman, 2008). The presence of cracks in the concrete cover must be accounted for if service life models are to represent conditions to which a concrete structure is exposed (Bentz et al., 2014, Lu et. al. 2013). In this study, reinforced mortar beams are cracked under three-point bending and then submerged in a solution of 1 mol/L sodium chloride (NaCl). After periods between 7 d and 21 d, the specimens are removed from the solution and cut perpendicular to the crack. Chloride concentration was determined using microbeam X-ray fluorescence spectrometry (µXRF). A support vector machine (SVM) algorithm was used to identify the cement paste and a generalized additive model (GAM) was used to interpolate the chloride counts over the scan domain. The results are compared to a mass balance model and show good agreement. The selection of the effective chloride binding reaction rate affects the simulation results by shifting the magnitude of the chloride concentration at a given depth. Selection of this parameter is important to service life calculations and is likely dependent on the physical and chemical properties of the cementitious system.

The model described in this work is an extension of the work of Bentz et al., 2014, Lu et. al. 2013, and Jones et al. 2015, where experimental measurements of the time-dependent transport properties of mortars are used as inputs to the model. Chloride measurements made at 25 μm intervals allow for a spatial resolution that is suitable for verifying modeling assumptions outlined in Bentz et al., 2014, Lu et. al. 2013, and Jones et al. 2015; specifically, the treatment of the transport properties around a crack can be assessed with this measurement technique.

MATERIALS AND METHODS

Cracked Mortar Beams

Mortar beams, measuring 4 cm x 4 cm x 16 cm were created with type I Portland cement. The cement used was Cement and Concrete Reference Laboratory (CCRL) material number 192 (January 2014). Chemical analyses were obtained from the consensus values available from CCRL (www.ccrl.us). Two water-to-cement ratios were studied, *w/c* = 0.4 and 0.5. These *w/c* values produce mortars with different effective diffusivities. Details of the mixture proportions using a blend of four sands are given in Table 1. All materials were weighed to the nearest 0.1 g.

Table 1. Mixture proportions in kg of material per total volume of materials (m^3)

	w/c = 0.4	*w/c* = 0.5
Cement	637.1	637.1
Water	254.8	318.6
ASTM F95 sand	357.1	357.1
ASTM Graded sand	271.4	271.4
ASTM 20-30 sand	271.4	271.4
ASTM GS-16 sand	528.5	528.5

A single section of threaded stainless steel rod was placed at the center of each beam and served as reinforcement of the specimen. In each beam, a crack was created by loading the specimen in 3-point bending after 7 d sealed curing. When the specimens reached an age of 28 d, they were removed from the curing chamber and placed in a 1 mol/L NaCl solution at 23 °C, until they were removed for μXRF analysis. After removal from the chloride solution, specimens were placed in a freezer at -10 °C at atmospheric pressure to slow subsequent diffusion. Samples were prepared for μXRF analysis by sectioning the beams into thirds and cutting perpendicular to the crack with a diamond saw. Cuts were made in 200-proof ethanol to limit the disruption of chloride ions. The surfaces to be scanned were polished with 120 grit SiC abrasive paper and ethanol.

Microbeam X-ray Fluorescence Spectrometry

μXRF settings and configuration

Chloride concentrations were determined from measurements made using a microbeam X-ray fluorescence spectrometer with a Rh X-ray source and a 25 μm thick Al primary beam filter. The X-ray tube voltage and current were set to 40 kV and 1000 μA, respectively. The nominal beam spot size was 50 μm, and the area measured was approximately 14 mm by 20 mm, centered on the crack. Measurements were made at 25 μm intervals, corresponding to an approximately half X-ray beam overlap, in a raster pattern. Spectra were acquired for 400 ms per location with the detector pulse shaping time set to 12.8 μs. X-Ray counts for Cl and other elements in the cement matrix were obtained from each spectrum by fitting peaks after background calculations and subtraction.

Calibration of μXRF data

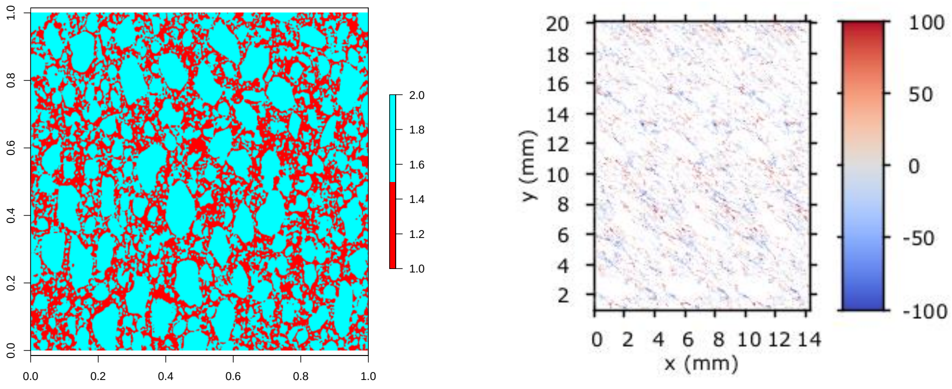
Calibration of μXRF data was achieved by preparing mortar specimens, composed of the same materials as the test specimens and in the same proportions, with known additions of chloride ions. The data output from the μXRF is in the form of a spectrum of counts *vs*. electron volts (eV) at each pixel. The counts in the range of 2.40 keV to 3.00 keV (corresponding to Cl Kα and Cl Kβ lines) at each pixel are fit to a log-normal distribution. The mean is computed and plotted versus the added chloride concentration with respect to total mortar volume. A simple linear model is assumed ($Y = \beta_1 X + \beta_0$), and the added chloride concentration is regressed onto the expected values of the counts. Initial regression analysis produced a β_0 = - 27 mol/m^3 and a standard error, SE = 32.5 mol/m^3. A hypothesis test suggested that β_0 is not statistically different from zero. The regression analysis was performed again with $\beta_0 = 0$ to produce the parameters shown in Table 2. Akaike's Information Criterion (AIC) suggests that the linear model with the intercept constrained to zero is best suited to predict the expected value of concentration (Wood, 2001, p.31). The estimate of β_1 in Table 2 has a low standard error and a *t*-statistic greater than the degrees of freedom (DOF) (*n* - 1), where *n* is number of samples. This indicates a relationship between the chloride concentration and the expected value of the counts, and it is estimated by the model $Y = \beta_1 X$.

Table 2. Coefficient estimates of linear model $Y = \beta_1 X$.

		Est. (mol/m^{3}count)	Std. Error (mol/m^{3}count)	*t*-statistic	*p*-value	DoF
w/c = 0.4	β_1	0.0378	2.4E-03	15.74	2.66E-07	8
w/c = 0.5	β_1	0.0356	2.3E-03	15.74	2.66E-07	8

Support Vector Machine and Generalized Additive Model

μXRF data was collected by rastering the sample under a stationary X-ray beam in an array with equally spaced points of 25 μm. The data of interest is the chloride ion concentration in the cement paste. Pixels from the coarse and fine aggregates, epoxy, as well as the interfacial transition zone around the aggregates were not included in the concentration model. Since cement paste contains Si, Ca and varying amounts of Cl, simple linear combination models are not sufficient to adequately segment the data. Further, the case of an analysis point that contains both cement and aggregate needed to be addressed. A training data set was collected from a mortar sample, of the same mix design, that contained no added chlorides (CCRL 192 contains 0.031 % by mass Cl) and was scanned under the same scan settings as the test specimens.



(a) Phase Identification by SVM

(b) Residuals of GAM

Figure 1. (a) Training data set produced by the SVM. The red indicates paste while the teal indicates aggregates. (b) Residuals of the GAM fit for the 2000 mol/m^3 Cl$^-$ standard. The scale limits are set to +/- 100 mol/m^3 to improve visualization of residual distribution.

This data set was used to train a support vector machine (SVM) to distinguish between two phases, aggregates and paste. The SVM does not rely on a linear combination of elemental compositions or on a defined count range. Rather, the model is able to separate out the data purely from the resulting X-ray spectrum, and, as a result, it is very efficient for processing the data and extracting the phase information. The resulting phase identification is given in Figure 1a, which shows the aggregates in cyan and the paste in red. The model can be adjusted to exclude the interfacial transition zones around the aggregates, but it was not able to account for aggregates that were smaller than the beam size of 50 µm. The SVM was used to produce a map of chloride counts only in the regions that contain paste. For this study, a generalized additive model (GAM), Equation 1, is used to interpolate the count over the domain.

$$\text{counts} = s(x) + s(y) + s(x,y) \qquad \textbf{(1)}$$

The functions s(x), s(y), s(x,y) are smoothing splines which serve as the basis for the GAM (James et al., 2013, p.282, Wood, 2011, p.121). A square root link function is used, and the number of knots required for the smoothing splines is determined by 3-fold cross validation. The residuals in Figure 1b are uniformly distributed about the domain indicating the probability of obtaining a certain error at a given point has a normal distribution. The result is a smooth representation of the chloride counts in the specimen.

Mortar Transport

To determine the transport properties required for simulations, several mortar mixtures were made for analyses of their pore solution resistivity, bulk resistivity, and chloride binding capacity. The time-dependent value of the mortar diffusivity can be estimated by monitoring the pore solution resistivity and bulk resistivity over time. Pore solution was extracted from mortar cylinders by the procedure described in (Barneyback and Diamond, 1981). The resistivity was measured by filtering the extracted pore solution through a 0.2 µm filter and using a resistivity cell, calibrated with KCl solutions of known conductivity (ed. Settle, 1997), to measure electrical impedance. The values were fit to the function shown in Equation 2. The assumed functional form of the diffusivity is given in Equation 3, where D(t) is found using Equation 4. Pore solution resistivity and mortar diffusivity coefficients are given in Table 3 with the corresponding plots given in Figure 2.

$$\rho_{ps} = C + A \cdot t^{b} \qquad \textbf{(2)}$$

$$D(t) = D_{\infty} + D_{i} \cdot t^{m} + D_{ib} \cdot t^{l} \qquad \textbf{(3)}$$

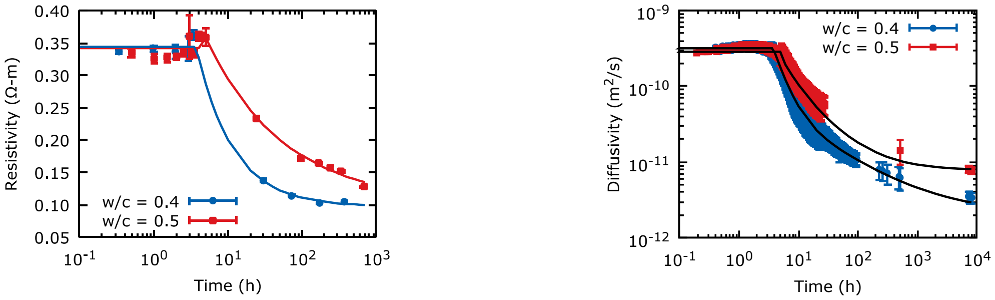
$$\rho_c/\rho_{ps} = D_0/D(t) \qquad \textbf{(4)}$$

Table 3. Curve fit parameters for pore solution resistivity and diffusivity of mortars

Parameter		Value	Std. Error
$w/c = 0.4$	C	0.0972 Ω-m	0.0034 Ω-m
	A	0.7805 Ω-m/s	0.0501 Ω-m/s
	b	-0.8782	0.0589
$w/c = 0.5$	C	0.1027 Ω-m	0.0143
	A	0.5022 Ω-m/s	0.0286
	b	-0.4193	0.0575

	Value	Std. Error
D_∞	2.143E-12 $\mathrm{m^2/s}$	1.92E-13 $\mathrm{m^2/s}$
D_i	6.910E-09 $\mathrm{m^2/s^2}$	2.09E-10 $\mathrm{m^2/s^2}$
D_{ib}	9.932E-11 $\mathrm{m^2/s^2}$	3.52E-12 $\mathrm{m^2/s^2}$
m	-2.467E+00	2.1E-02
l	-5.37E-01	1.2E-02
D_∞	7.821E-12 $\mathrm{m^2/s}$	4.20E-13 $\mathrm{m^2/s}$
D_i	3.487E-09 $\mathrm{m^2/s^2}$	2.54E-10 $\mathrm{m^2/s^2}$
D_{ib}	4.868E-10 $\mathrm{m^2/s^2}$	6.95E-11 $\mathrm{m^2/s^2}$
m	-2.113E+00	9.7E-02
l	-8.424E-01	3.8E-02

To improve the numerical stability of the finite element (FE) model, the data in Figures 2a and 2b were fit to Equations 2 and 3 using a non-linear least-squares regression routine. Equation 3 is used to determine the bulk diffusivity at a given time point. The very early age diffusivity (t < 3.5 h for *w/c* = 0.4 and t < 5 h for *w/c* = 0.5) is assumed to be constant as the changes in pore solution and bulk resistivity are relatively small over these time periods. The parameters used in the finite element model are given in Table 3. The absolute value of m in equation 3, for both *w/c* = 0.4 and 0.5 is greater than 1. Bentz et al., 2000, mention that a value greater than 1 cannot be used with an analytical solution, but Equation 3 has been employed for a numerical approach. The curve of the fitted diffusivity values is given in Figure 2b, which shows the proper decrease in diffusivity with time in the time period of interest. An important component to modeling chloride ion concentration is the effects of physical absorption to and chemical reaction with the cement matrix. This is accomplished by a procedure given by Luping and Nilsson, 1993. After 28 d of sealed curing, the mortar was ground to a powder and passed through a sieve with a 1680 µm opening. The chlorides bound to the cement paste per kg of cement are given in Figure 3 for both *w/c* = 0.4 and *w/c* = 0.5. Table 4 gives the coefficients of a Langmuir isotherm determined from a non-linear regression.

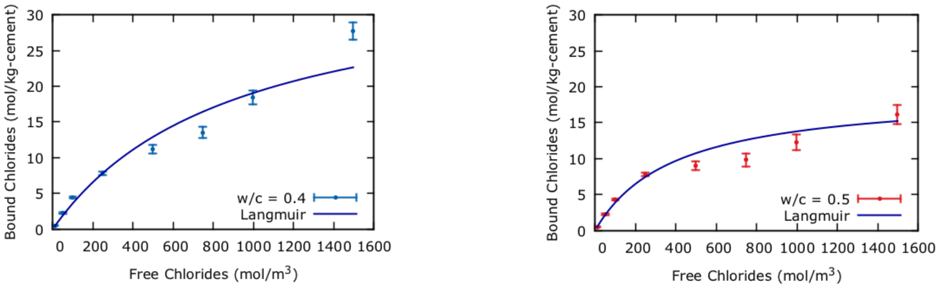


(a) Pore Solution Resistivity (b) Mortar Diffusivity

Figure 2. (a) Plot of measured pore solution resistivity. (b) Plot of the estimated diffusivity of the mortar determined from the non-linear regression in (a) and the measured mortar resistivity. The solid lines in (a) and (b) are the curves resulting from non-linear regression. Error bars represent the 95 % confidence interval of the measured data.

Table 4. Parameters determined from non-linear least squares regression of Langmuir isotherms of chloride binding measurements.

Isotherm		*w/c* = 0.4		*w/c* = 0.5	
		Value	Std. Error	Value	Std. Error
Langmuir	*α*	4.01E-02	6.4E-03	4.890E-02	2.2E-04
	β	1.10E-03	4.0E-04	2.54E-03	3.6E-04



(a) *w/c* = 0.4 (b) *w/c* = 0.5

Figure 3. Chloride binding isotherms for (a) *w/c* = 0.4 mortar and (b) *w/c* = 0.5 mortar. Bound chlorides are plotted as the number of moles of chloride ions bound per kg of cement in the mixture. Chloride binding in these plots is assumed to be the sum of physically absorbed chloride ions and ions consumed in Friedel's salt formation. Error bars represent the 95 % confidence interval.

Mass Balance Model

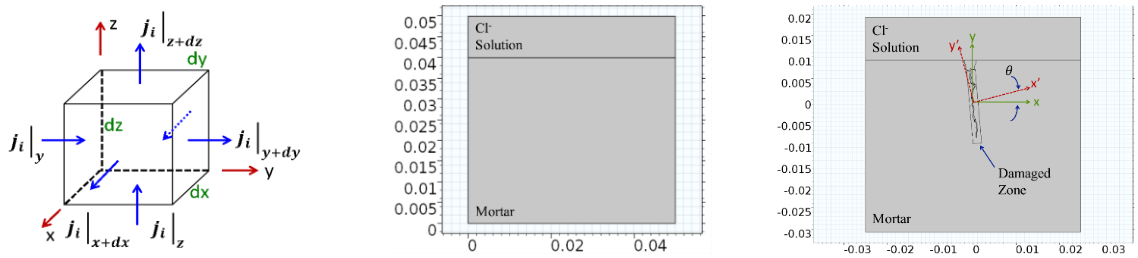
Transport of chloride ions through the paste matrix (cement and water) is derived from a mass balance on an infinitesimal volume of the domain of interest, shown schematically in three dimensions in Figure 4a. Formulating the governing equations in the paste is equivalent to assuming that the aggregates do not absorb or transport chloride ions through them. Within the paste, chloride transport is assumed to occur through the water saturated pore structure. The flux across a face of the control volume is $\mathbf{j_i} = D_{con}(t)\nabla C_{f\text{-pore}} = \varepsilon_p D_{con}(t)\nabla C_f$ where $C_{f\text{-pore}}$ is expressed in terms of water accessible pore volume and C_f is expressed in terms of paste volume. The time rate of change of the chloride concentration in the paste volume is equal to the sum of the flux going into the volume minus the flux leaving the volume plus accumulations of chlorides inside the volume. This is expressed mathematically in Equation 5 where Fick's Law is used to relate the flux to the free chloride concentration (C_f). In Equation 5, the binding of free chlorides to the mortar matrix is modeled as a first order reaction with reaction rate k. The water accessible porosity of the paste is ϵ_p. The change in concentration of bound chlorides (C_{bound}) is described by Equation 6, where ($C_{bound\text{-}eqbm}$) is the equilibrium concentration of bound chlorides.

$$\frac{\partial C_f}{\partial t} = \nabla \cdot \left(\epsilon_p D_{con}(t) \nabla C_f\right) + k\left(C_{bound} - C_{bound-eqbm}\right) \qquad \textbf{(5)}$$

$$\frac{dC_{bound}}{dt} = \epsilon_p k\left(C_{bound-eqbm} - C_{bound}\right) \qquad \textbf{(6)}$$

$$C_{bound-eqbm} = \alpha C_f/(1 + \beta C_f) \qquad \textbf{(7)}$$

The relationship between the free chloride concentration and the concentration of chlorides that will react with the cement paste, at equilibrium, is described by the Langmuir isotherm, Equation 7. Two domains are used in the simulations. Figure 4b shows the control, un-cracked case while Figure 4c, shows a representation of a cracked case where the crack geometry is imported into the model from the µXRF images.



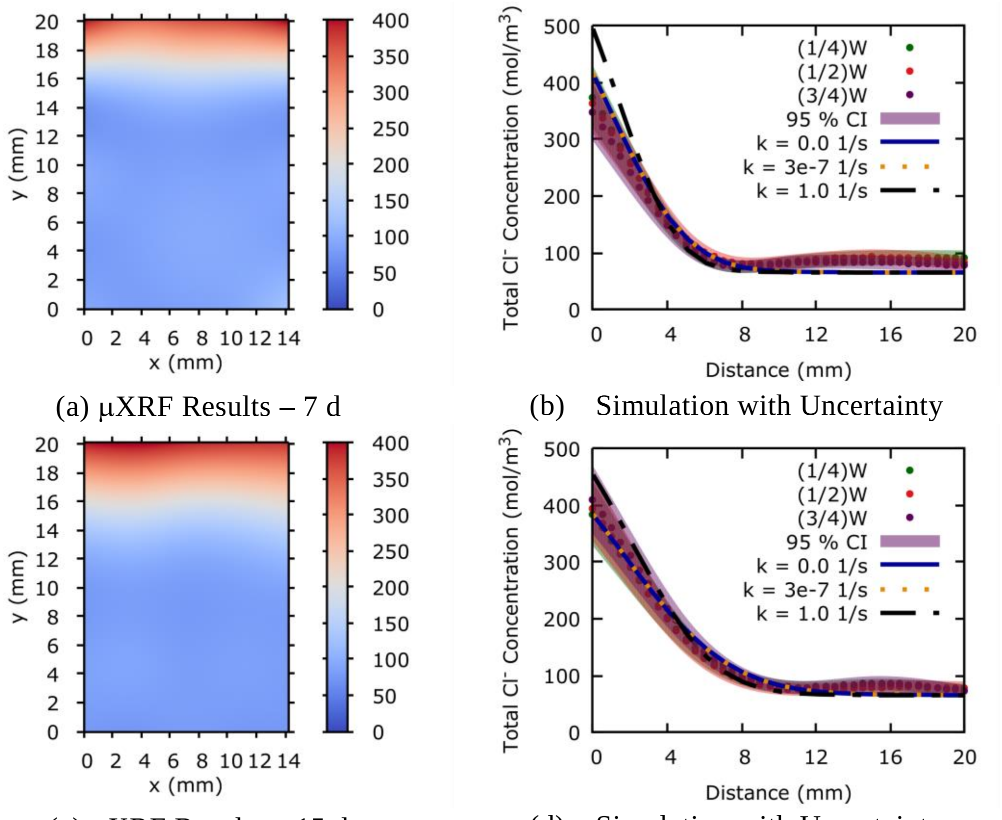
(a) Control Volume (b) Un-cracked Case (c) Cracked Case

Figure 4. (a) Schematic representation of the infinitesimal control volume, (b) the domain representing the un-cracked case, and (c) cracked case (units: m).

RESULTS AND DISCUSSION

Control Case – No Crack

A domain without a crack is modeled as a control case. This scenario is considered the "best case" for protection of the rebar from corrosion and serves as a reference for the ability of the model to predict chloride ion concentration. Figures 5a-b and Figures 5c-d show results of a specimen exposed to a 1 mol/L NaCl solution for 7 d and 15 d, respectively. Figure 5a shows the results of the µXRF scan and Figure 5b shows the results along three lines, from y = L to y = 0, across the domain. The shaded region of the plot in Figure 5b is the measurement uncertainty at a 95 % CI, as determined by the procedure described in JCGM 101:2008. Figure 5 shows good agreement between the model and the measured results of the μXRF scans. In Figure 5b, the model is within the measurement uncertainty. A similar result is observed in Figures 6a-d. The model agrees well with the μXRF data near the top surface in Figure 6b but underestimates the measured values as the distance increases. This may be a result of the calibration procedure. In Figure 6d, there appears to be an inflection point in the measured data at 4 mm. Upon closer inspection of the sample, there appears to be a void just below the surface which will affect the counts. However, the model does follow the general trend of the measured data. The results in Figure 5a-d (and 6a-d) exhibit good agreement between the model and measured data. The chloride binding reaction rate, k, is assumed to be an effective reaction rate which includes both physical absorption of chloride ions onto calcium silicate hydrate (C-S-H), as well as the formation of reaction products such as Friedel's salts. In previous modeling studies, the chloride binding reaction rate was assumed to be 3.0E-07 1/s (Jones et al., 2015, Bentz et al., 2013). The concentration in the storage solution was measured at intervals of approximately 24 h for the first 3 d and then approximately 7 d thereafter. It was observed that the chloride binding experiments reached their equilibrium states within 2 d, corresponding to a reaction rate of approximately 5.7E-06 1/s. Since the time to equilibrium of the chloride binding experiments is a function of the particle size of the ground mortar, it is likely that this effective reaction rate would be much slower in a system where chlorides are diffusing though a pore structure, as the surface area available for chloride binding would be much lower.



(a) μXRF Results – 7 d

(b) Simulation with Uncertainty

(c) μXRF Results – 15 d

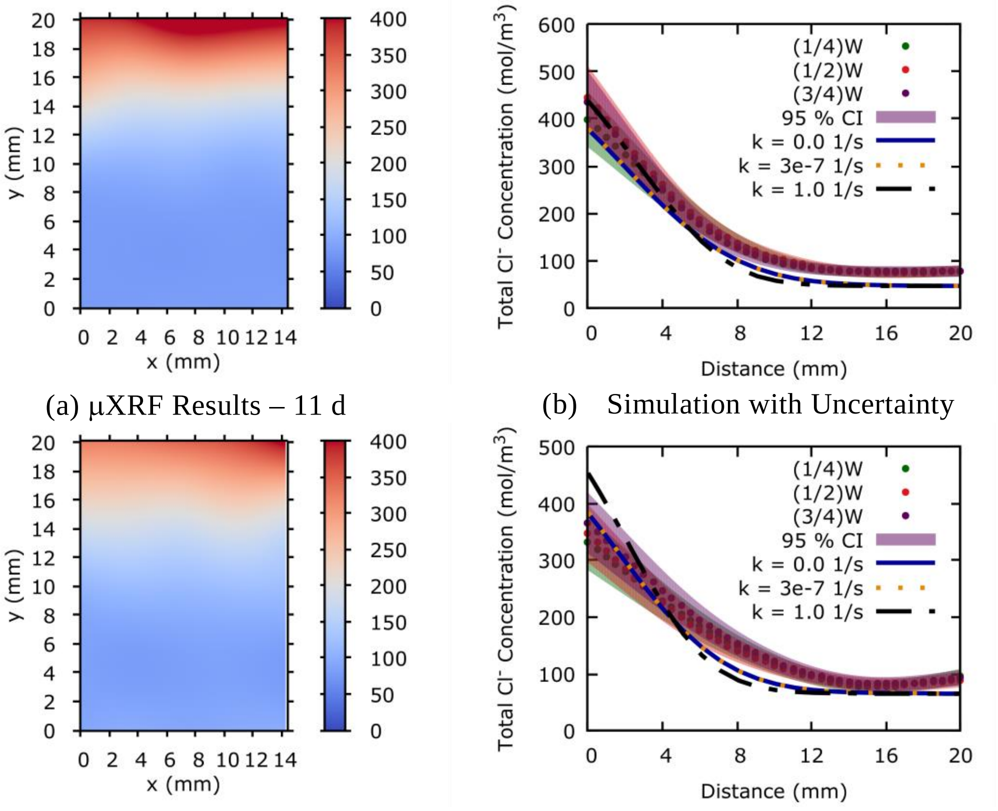
(d) Simulation with Uncertainty

Figure 5. Total Chloride ion concentration in control specimen of *w/c* = 0.4 at 7 d exposure (a) & (b) and 15 d exposure (c) & (d) as measured by μXRF, (a) & (c), and solution to eq. 5 & 6, (b) & (d). The concentration measured from the top, exposed surface and the measurement uncertainty at a 95 % confidence interval is shown. "W" is the maximum x-direction value. Concentration is expressed in moles per m^3 of mortar.

To study the influence of k, the simulations were run with k = 1.0 s^{-1}, 3.0E-07 s^{-1}, and 0 s^{-1}. Figures 5b and 5d (and Figure 6b and 6d) demonstrate the influence of the effective chloride binding rate on the simulation results. Simulation results indicate that the model is not sensitive to the reaction rate so long as the time steps taken by the solver are long enough to allow for the binding reaction to reach equilibrium. The μXRF results suggest that chloride binding is happening at a rate closer to the assumed value of 5.7E-06 1/s. When the reaction rate is reduced, the influence of the chloride binding is reduced – $k \rightarrow 0$ removes the chloride binding term from Equation 5. This result indicates the need for a better measurement of chloride binding kinetics and suggests a first-order reaction rate may not be an appropriate approximation. Still, the simulation results are within the measurement uncertainty indicating the simulation may provide a suitable estimation of chloride concentration at a given position and time. Deviation of the measured values from simulation results may be explained by increased porosity due to leaching of portlandite and decalcification of C-S-H resulting from hydrolysis of the cement paste (Carde and Francois, 1997). This change in the matrix will affect X-ray counts due to changes in grain sizes that are a result of the increased porosity (Jenkins and De Vries, 1975).

Saturated Crack Case

Simulations of cracked mortar are performed as in the control case but with a few important modifications to the model. The crack geometry is imported to the FE software by combining the Si and Ca μXRF images, converting them to a binary image, and then adjusting the threshold such that only the crack outline is visible (Figure 4c).



(a) μXRF Results – 11 d (b) Simulation with Uncertainty

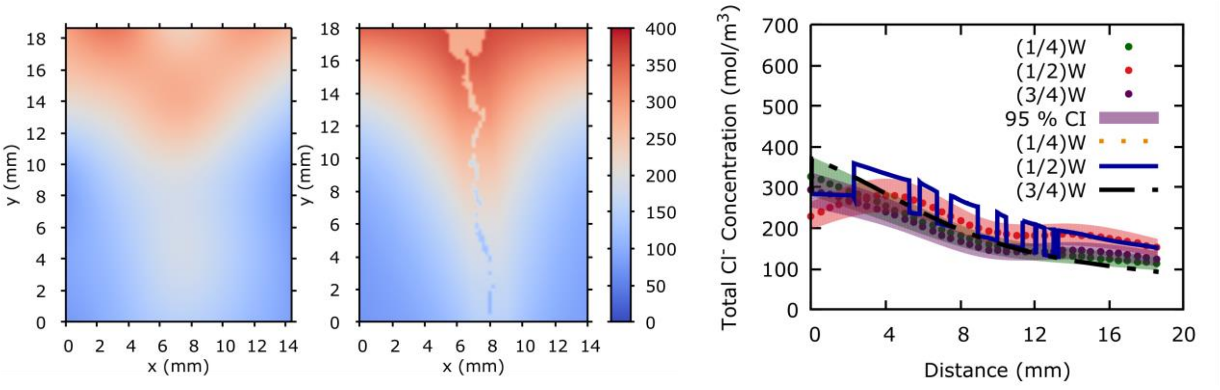
(c) μXRF Results – 21 d (d) Simulation with Uncertainty

Figure 6. Total Chloride ion concentration in control specimen of *w/c* = 0.5 at 11 d exposure (a) & (b) and 21 d exposure (c) & (d) as measured by μXRF, (a) & (c), and solution to eq. 5 & 6, (b) & (d). The concentration measured from the top, exposed surface and the measurement uncertainty at a 95 % confidence interval is shown. "W" is the maximum x-direction value. Concentration is expressed in moles per m^3 of mortar.

Previous studies attempting to simulate chloride concentration around cracks have assumed that a region around the crack has diffusivity properties that are different from the bulk. Jones et al., 2015 and Bentz et al., 2013 assumed this region to be approximately 4 mm from the crack edge. This assumption was based on experimental evidence reported in Şahmaran and Yaman, 2008 and the chloride maps presented in Figure 7a and Figure 8a support these findings, as the depth of penetration from the crack surface appears to be greater than that from the top, exposed surface. Following the simulation procedures outlined in Jones et al., 2015 and Bentz et al., 2013, the chloride profile for two cracked domains are simulated by solving Equations 5 through 7. The crack in the sample tends to deviate from vertical. To account for this phenomenon, the damaged zone region was rotated around its center point to align with the crack. Since Equation 5 is formulated assuming the principal directions of the flux are in line with the x and y axes, a rotation is applied to the diffusivity tensor which produces components $D_{xx} = D_{yy} = DF \cdot D(t)\cos(\theta)$ and $D_{xy} = -D_{yx} = -DF \cdot D(t)\sin(\theta)$ where DF is a parameter used to estimate the increase in diffusivity. The parameter DF is thought to be a result of increased porosity around the crack possibly due to micro-cracking. Figure 7a shows the chloride concentration as measured by μXRF and Figure 7c shows the concentration as a function of depth with (1/2)W approximately centered on the crack, where the symbols represent measured results and the lines represent simulation results. The simulation was run with DF = 1, 10, and 20 and the width of the damaged zone = 1 mm (1.5 mm for *w/c* = 0.5). The convergence of the simulation to the μXRF results improved as DF increased to 10 for *w/c* = 0.4 and 20 for *w/c* = 0.5. The simulation results in Figure 7 are shown with DF = 10 and agree well with the measured μXRF results. Increasing DF to 20 produced results that exceeded measured values near the crack tip.

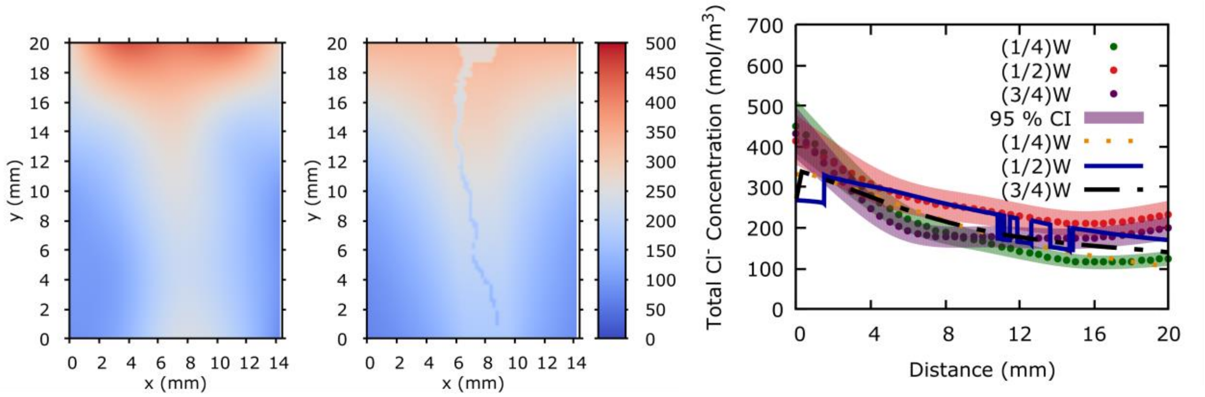
The model predicts the chloride concentration near the top and bottom of the scanned area but tends to over predict measured chloride concentrations near the middle. The dips in the simulation result from regions where the model results are in the crack domain, which does not bind chlorides. Figure 8 shows the results for a crack in a *w/c* = 0.5 mortar with DF = 20 in a region around the crack. The simulation results in Figure 8 agree well with the μXRF results but do not appear to capture the behavior near the top surface. This is likely due to positional errors introduced into the model when converting the Si and Ca μXRF images into a format that can be accepted by the model. However, the behavior away from the top surface is in agreement with the μXRF measurements and is therefore a suitable approximation to the observed measurements.

Figures 7 and 8 present a comparison between experimental measurements of chloride concentration and simulation results. Jones et al. 2015, performed a series of simulations, which attempted to model the chloride concentration around rectangular cracks. Based on the work of Şahmaran and Yaman, 2008, a region around the crack was defined to have a diffusivity approximately 20 times the bulk diffusivity.



(a) μXRF Results (b) Simulation Results (c) Simulation with Uncertainty

Figure 7. Total Chloride ion concentration in cracked specimen (*w/c* = 0.4 crack at 14 d exposure, DF = 10) as measured by (a) μXRF and (b) & (c) solution to eq. 5 & 6. The concentration measured from the top, exposed surface and the measurement uncertainty at a 95 % confidence interval is shown in (b). "W" is the maximum x-direction value.



(a) μXRF Results (b) Simulation Results (c) Simulation with Uncertainty

Figure 8. Total Chloride ion concentration in cracked specimen (*w/c* = 0.5 crack at 15 d exposure, DF = 20) as measured by (a) μXRF and (b) & (c) solution to eq. 5 & 6. The concentration measured from the top, exposed surface and the measurement uncertainty at a 95 % confidence interval is shown in (b). "W" is the maximum x-direction value.

Based on the work of Şahmaran and Yaman, 2008, a region around the crack was defined to have a diffusivity approximately 20 times the bulk diffusivity. Chloride concentration measurements were made on the extraction fluid of powdered mortar that was obtained by drilling to known depth. This measurement technique produces an estimate of the diffusivity for the region sampled by the coring bit. With an approximate spatial resolution of 25 μm – it should be noted that the X-ray beam spot size is 50 μm, so in this study, spatial resolution indicates the approximate edge size of one pixel in the data set – the transport properties can be assessed at smaller length scales. With this enhanced measurement technique, Figures 7 and 8 indicate that DF is variable and is dependent on the crack geometry. The model detailed in this study addresses crack orientation by aligning the principal directions of the diffusivity tensor with the crack. These two factors improved convergence between experimental measurements and simulation results as shown in Figures 7c and 8c.

CONCLUSIONS

In this study, experimental and modeling procedures are detailed to measure the chloride concentration around a crack created in a reinforced mortar beam. Measurements are made on samples with and without a crack, for *w/c* = 0.4 and *w/c* = 0.5 mortars. Simulation results are within the measurement uncertainty when the uncertainty is derived using a Monte Carlo method for simulating data. Using the FE simulation to conduct a parametric study of the effective chloride binding reaction rate indicates that the value of the parameter can be estimated from the time it takes the chloride binding experiments to reach equilibrium. When a crack is present in the domain of interest, a region around the crack is defined to have a diffusivity 10 or 20 times greater than the bulk mortar, depending on the mortar *w/c*. Orienting this region in the direction of the crack and conducting a parametric study of the DF factor produced results that were within the uncertainty of the μXRF measurements. The results presented in this paper demonstrate the deleterious effect of a crack on the protection capacity of a cementitious cover over a steel bar. The model presented is able to predict chloride concentrations when given the appropriate inputs for the material under investigation. Experimental measurements taken with a spatial resolution of approximately 25 μm over an approximately 14 mm x 20 mm domain allow for model verification at spatial increments suitable for studying the DZ diffusivity. A better prediction of chloride concentration near cracks will improve service life models by moving the model closer to real-world conditions.

REFERENCES

Barneyback Jr., R.S., and Diamond, S. (1981) Expression and Analysis of Pore Fluids from Hardened Cement Pastes and Mortars. *Cement and Concrete Research*. 11 (2). p. 279-285.

Bentz, D.P., Feng, X., & Hooton, R.D. (2000) Time-dependent diffusivities: possible misinterpretations due to spatial dependence. *Testing and Modeling the Chloride Ingress into Concrete. Proceedings. 2nd International RILEM Workshop.* September 11-12, Paris, France, p. 225-233.

Bentz, D.P., Garboczi, E.J., Lu, Y., Martys, N., Sakulich, A.R., & Weiss, W.J. (2013) Modeling of the influence of transverse cracking on chloride penetration into concrete. *Cement and Concrete Composites*. 38. p.65-47.

Bentz, D.P., Guthrie, W.S., Jones, S.Z., and Martys, N.S. (2014) Predicting Service Life of Steel Reinforced Concrete Exposed to Chlorides: A discussion of real-world considerations for effective modeling, *Concrete International*. 36 (9). p. 55-64.

Carde, C., and Francois, R. (1997) Effect of ITZ leaching on durability of cement-based materials. *Cement and Concrete Research.* 27(7). p. 971-978.

James, G. et al. (2013) *An Introduction to Statistical Learning with Applications in R.* NY: Springer.

JCGM 101:2008; *Evaluation of measurement data – Supplement 1 to the "Guide to the expression of uncertainty in measurement" – Propagation of distributions using a Monte Carlo method*; Joint Committee for Guides in Metrology (JCGM) (2008).

Jenkins, R. and De Vries, J.L. (1975) *Practical X-Ray Spectrometry*. New York: Springer-Verlag p. 118

Jones, S.Z., Martys, N.S., Lu Y., Bentz, D.P. (2015) Simulation Studies of Methods to Delay Corrosion and Increase Service Life for Cracked Concrete Exposed to Chlorides. *Cement and Concrete Composites* 58 p.59-69.

Lu, Y., Garboczi, E.J., Bentz, D.P., and Davis, J.M., Modeling Chloride Transport in Cracked Concrete: A 3-D Image-Based Microstructure Simulation, *Proceedings of the 2012 COMSOL conference, Boston*, MA, 2012

Luping, T., Nilsson, L.O., (1993) Chloride binding capacity and binding isotherms of OPC pastes and Mortars. *Cement and Concrete Research* 23 (2). p.247-253.

Mills, R. & Lobo, V.M.M. (1989) Self-Diffusion in Electrolyte Solutions. New York: Springer.

Şahmaran, M., & Yaman, İ. Ö., (2008) Influence of transverse crack width on reinforcement corrosion initiation and propagation in mortar beams. *Canadian Journal of Civil Engineering* 35 (3). p.236-245.

Samson, E., Marchand, J., Snyder, K.A., & Beaudoin, J.J. (2005) Modeling Ion and Fluid Transport in Unsaturated Cement Systems in Isothermal Conditions. *Cement and Concrete Research* 35 (1). p.141-153.

Settle, F (ed.) 1997, *Handbook of Instrumental Techniques for Analytical Chemistry*, Prentice Hall, New Jersey, p.760.

Vu, H.Q., Stitmaannaithum, B., & Sugiyama T. (2013) Prediction of Chloride Profile at Crack Location in Reinforced Concrete Under Flexural Loading. *ASEAN Engineering Journal Part C.* 2 (1).

Wood, S.N. (2011) *Generalized Additive Models An Introduction with R.* New York: CRC Press.

An Overview of a Smart Manufacturing System Readiness Assessment

Kiwook Jung[1], Boonserm Kulvatunyou[1], Sangsu Choi[2], and Michael P. Brundage[1]

[1]Engineering Lab, National Institute of Standards and Technology (NIST)
Gaithersburg, MD, USA
[2]IGI, LLC. Clarksburg, MD, USA
{kiwook.jung, serm, mpb1}@nist.gov
Sangsu.choi@igiamerica.com

Abstract. Smart manufacturing, today, is the ability to continuously maintain and improve performance, with intensive use of information, in response to the changing environments. Technologies for creating smart manufacturing systems or factories are becoming increasingly abundant. Consequently, manufacturers, large and small, need to correctly select and prioritize these technologies correctly. In addition, other improvements may be necessary to receive the greatest benefit from the selected technology. This paper proposes a method for assessing a factory for its readiness to implement those technologies. The proposed readiness levels provide users with an indication of their current factory state when compared against a reference model. Knowing this state, users can develop a plan to increase their readiness. Through validation analysis, we show that the assessment has a positive correlation with the operational performance.

Keywords: smart manufacturing readiness, smart factory, maturity model

1 Introduction

Manufacturers lack a concrete methodology to choose and prioritize emerging technologies that aid in the creation of smart manufacturing systems and factories. On top of this, manufacturers may need to implement organizational and process improvements to realize the full benefits from these technologies. Fig. 1 shows a survey result indicating that most manufacturers have trouble making such improvements. While larger companies can bring in consultants to assist with such issues, small and medium size manufacturers typically do not have the funds to do the same.

Existing methods such as the Supply Chain Readiness Level [2] and MESA Manufacturing Transformation Strategy [3] exist, but they largely ignore the use of information and communication technologies (ICT) as a primary foundation for making those improvements. There are existing works, which study the impact of Information Technology (IT) adoption to businesses (also known as business & IT alignment). However, each study typically focuses on evaluating a single technology such as the Enterprise Resource Planning (ERP) system or Manufacturing Execution System

adfa, p. 1, 2011.
© Springer-Verlag Berlin Heidelberg 2011

(MES). These studies have not taken into account other aspects of the organization that can affect the impact of the respective technology adoption.

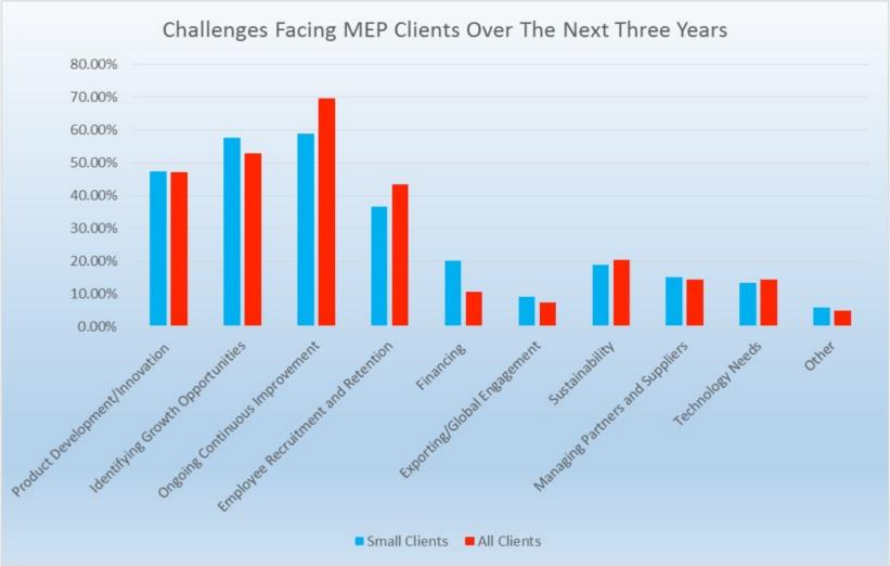


Fig. 1. Survey result highlighting Ongoing Continuous Improvement as the challenge faced by most manufacturers [1]

This paper describes our initial work to develop a method for assessing a factory's readiness for incorporate emerging ICT technologies to become a smart factory. In our view, a smart factory uses ICT to maintain and improve its operational performance in response to its changing environment. Consequently, the method breaks down the assessment into four maturity components including the IT, the information connectivity, organization, performance management program maturities. Our method then combines these assessments into a single Smart Manufacturing System Readiness Level (SMSRL) index, which can be used for benchmarking individual factories or as criteria for selecting a supplier among several factories. In addition to describing our method, we discuss a correlation analysis that we performed. That analysis shows that the SMSRL index has a positive correlation with the operational performance.

Next we discuss related work in more detail before describing the SMSRL assessment method. Then, the result from the validation study is presented and a conclusion and remarks are given.

2 Related Work

Several types of readiness levels are used within the manufacturing sector. **Technology** Readiness Level (TRL) indicates the maturity of a technology for commercial adoption [4]. Similarly, **Manufacturing** Readiness Level (MRL) indicates the maturity of a manufacturing process technology [5]. An organization can use the same scale to indicate the maturity/capability of its respective technology as well. These methods do not evaluate a particular company for its readiness to adopt a particular technology.

Supply Chain Readiness Level (SCRL) [2] provides a method to assess the ability of the supply chain to operate and to achieve specific operational performance targets. The readiness levels are associated with characteristics within fifteen (15) categories that discretely provide an improvement roadmap for a supply chain design and the operation. Similar to the TRL and MRL, SCRL does not provide a methodology for a particular organization to assess its readiness to adopt a particular technology, which may correspond to some categories of the characteristics.

The MESA manufacturing transformation strategy (MTS) provides a framework based on the ISA-95 standard [3] to prepare an organization for Manufacturing-Operation Management (MOM) technologies adoption in four (4) business domains including Business Processes, Organization Structure, Personnel Skill Sets, and Manufacturing System Technology.

The SMSRL assessment objective is similar to that of the MESA-MTS albeit with the scope going beyond MOM technologies. Technically, the SMSRL index provides an indication of the current state with respect to a reference model. Both the SMSRL and the MESA-MTS allow the reference model to evolve as new technologies emerge and become available. Because of this, the assessment piece of the method, by design, is kept independent of the reference model.

3 Method

Fig. 2 provides an overall architecture of the readiness level assessment. It summarizes the steps, the inputs, and the outputs involved in the assessment followed by improvement plan development. The process is iterated after the plan has been implemented. The primary purpose of the proposed assessment based on the SMSRL index is to 1) help manufacturers determine their current level and 2) develop a customized improvement plan.

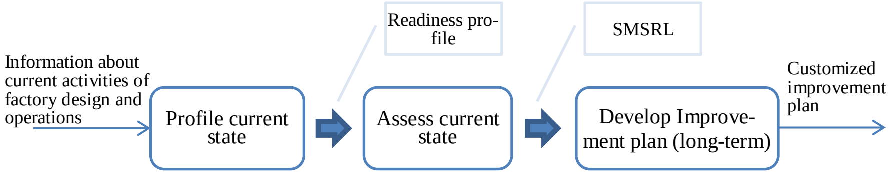

Information about current activities of factory design and operations
Profile current state
Readiness profile
Assess current state
SMSRL
Develop Improvement plan (long-term)
Customized improvement plan

Fig. 2. Overall assessment framework

3.1 Profiling the Current State

The SMSRL proposed in this paper is based on the Factory Design and Improvement (FDI) reference-activity model defined in [6]. That model provides a set of reference activities; information entities for input, output, and constraints on each activity; and relevant software functions using the IDEF0 functional requirement modeling method [7]. On the basis of this model, we developed a questionnaire for profiling [8]. It is to be answered by relevant factory personnel. The questionnaire is organized into four measurement dimensions (C1 to C4) each of which consists of measurement items (process, designated personnel, etc.) as shown in Fig. 3. See the citations in **Error! Reference source not found.** for the sources of these dimensions. Next we discuss each dimension in more detail.

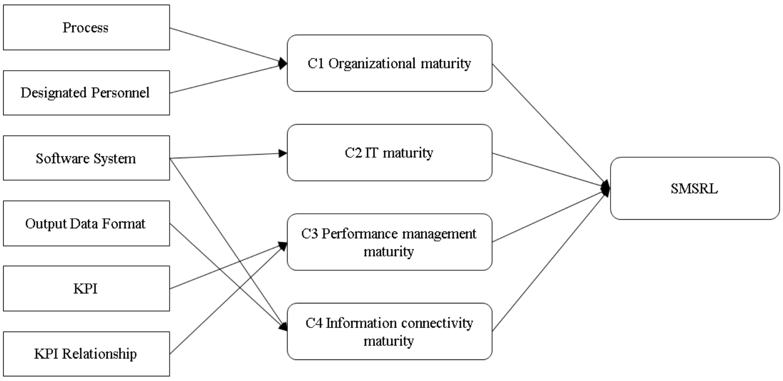


Fig. 3. SMSRL measurements

The Organizational maturity dimension (C1) is conceptually defined as the comprehensiveness of the activities in the reference activity model performed by the manufacturers. It is measured by 1) whether there is a process that formally manages each activity; and 2) whether there is a responsible human resource assigned to the activities.

The IT maturity dimension (C2) is conceptually defined as the degree to which IT resources are available and working. The IT resources refer to computerized tools and methods. For example, a paper-based analysis method for layout design would not be qualified as an IT resource.

The Performance Management maturity dimension (C3) is conceptually defined as the degree to which the performance measures are used and monitored. This dimension also takes into account the connectivity between different operational performance measures where appropriate.

Lastly, the Information connectivity maturity dimension (C4) is conceptually defined as the maturity of the method to exchange the required information and the degree to which the information is shared/exchanged.

Profiling the current state consists of three operations: scope determination, information collection and consolidation. The scope is represented by relevant activities and stakeholders. The FDI model also indicates stakeholders relevant to each activity based on the ISA-88 manufacturing control architecture [9]. Information collection and consolidation are performed collaboratively among the group of stakeholders that are relevant to the scope.

3.2 Evaluate Current State

The evaluation of the current state compares the profile to the reference activity model. Computation methods, as shown in Table 1, are applied to each measurement dimension resulting in quantitative measures that can be used for comparison and benchmark.

Table 1. Computation Methods for SMSRL

SMSRL Construct	Computation Method
C1: Organizational maturity [10]	Counting measure, Activity maturity scoring scheme
C2: IT maturity [11]	Counting measure
C3: Performance management maturity [12]	Counting measure
C4: Information connectivity maturity [13]	Incidence matrix-based similarity measure, Incidence scoring scheme

The counting measure is the ratio between the number of elements employed in the current practice and those suggested in the reference activity model. For example, the number of software functions (per the reference model) available in the factory divided by the number of all the software functions identified in the reference model gives a C2 measure.

The Activity maturity scoring scheme is based on the Capability Maturity Model Integration (CMMI) [14]. The stakeholder of each activity scores the maturity of the activity based on the scale shown in Table 2.

Table 2. Activity maturing scoring scale

Linguistic scale	Task score	Characteristics
Not performed	0	-
Initial	1	Processes established, but unpredictable
Managed	3	Processes characterized for projects
Defined	5	Process characterized for the organization
Qualitative	7	Processes measured and controlled
Optimizing	9	Focus process improvement

The incidence matrix is commonly used to represent and analyze interactions between entities in a complex system. Here, an incidence matrix is used to represent the information entities connected between activities; and as such can be used to quantify the information connectivity maturity (C4). It is an n x n matrix where n is the number of activities under evaluation, the row is the activity that provides the information entity (from-activity or sender activity), and the column is the activity taking the information entity as an input (to-activity or receiver activity). The cell, the incidence, indicates the maturity of the information flow from the row to the column. Table 3 shows a schematic view of an incidence matrix. The maturity of the information flow is marked by the scoring scheme shown in Table 4 with the highest score (1) being connected by a standard data exchange. All reference incidence matrices assume the highest score where there is the information connectivity between the from- and to-activity. A score of 0.7 represents that software capability for data exchange among activities exists, but information is not currently exchanged. When the data is exchanged manually between activities, the score is 0.3. A score of zero indicates that there is no data exchange between the activities.

Table 3. Activity incidence matrix

From/To	**To Act$_1$**	**…**	**To Act$_j$**
From Act$_1$	inc$_{11}$	…	inc$_{1j}$
…	…	…	…
From Act$_i$	inc$_{i1}$	…	inc$_{ij}$

Table 4. Incidence scoring scheme

Incidence Score	**Scoring Rule**	**Definition**
1	if $a \in (S_j \cap B_m)$ then, $c = 1xRef$	Standard data formats for activity *j* (and) compatible data formats for software system *m*
0.7	if $a \in B_m$ then, $c = 0.7xRef$	Compatible data formats for software system *m*
0.3	if $a \notin B_m$ then, $c = 0.3xRef$	Manual transformation required from output data *a* to compatible data formats for software system *m*
0	if $Ref = 0$ then, $c = 0xRef$	No exchange required
0	If i $or\ j = \emptyset$ then, $c = 0xRef$	The current state does not perform the activity *i* or *j*. to be performed
0	If i=j then, $c = 0xRef$	Recursive
Where *i* is the sender activity; *a* is the output data format of the activity *i*; S_j is a set of standard data formats associated with the receiver activity *j*; B_m is a set of compatible data formats for the receiver software system *m*; and *c* is the incidence score.		

The evaluation result can be visualized as shown in Fig. 4. Each indicator can be used individually or combined into a single SMSRL index. For simplicity, a single SMSRL index was computed using an average of C1, C2, C3 and C4. The overall index and/or individual construct can be used to prioritize the factory improvements or to evaluate potential suppliers.

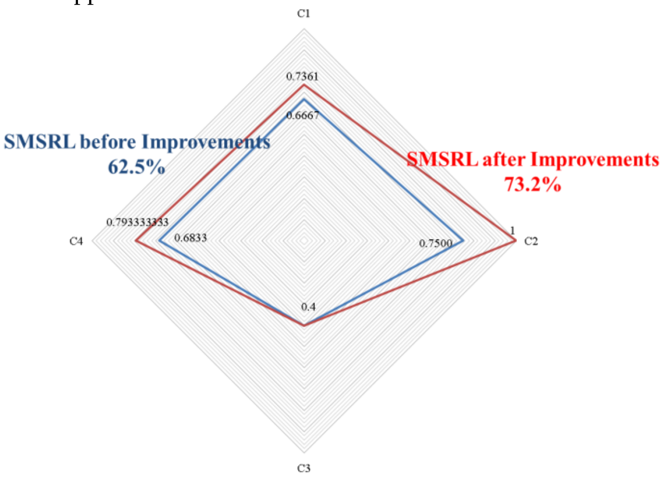


Fig. 4. An exemplary assessment result

3.3 Develop improvement plan

In the last step, the evaluation result is used to develop and prioritize an improvement plan. A classification analysis shown in the next section provides a high-level improvement recommendation. Our future work lies in developing a method to provide a more detailed recommendation.

4 Validation Study

This section investigates the validity of the proposed assessment using a similar approach to [13]. First, data about the relationships between the SMSRL and operational performance was collected. Then, hypothesis tests for the statistical significance of the relationships were performed. Lastly, we analyzed patterns of the SMSRL that can guide an improvement plan development. These activities are explained below.

4.1 Data used for the validation

Existing studies in the domain of business and IT alignment were used for the validation. A detailed analysis on the existing studies can be found in [8]. Different alignment constructs (i.e., measurement items) from these studies were mapped to performance categories (e.g., operational, financial) and were statistically correlated using empirical data.

4.2 Validation method

To establish the relationship between the SMSRL assessment and the performance categories, the measurement items of the SMSRL assessment are mapped to those considered in the studies (operational, financial, value-based, and overall). A similarity value between the SMSRL assessment and the target study is then calculated using the n-gram measure (intersection divided by union). This gives the basis for the correlation analysis shown in the next subsection.

4.3 Hypothesis test

Four hypothesis tests were performed. Statistically significant, positive-correlations with the SMSRL index were found on the operational performance, overall performance, and value-based performance as shown in Table 5. The financial performance was not found (hence not shown) to have a statistically significant positive-correlation.

Table 5. Hypothesis test results

Hypothesis	Pearson Cor.	Sig
H1: the higher the similarity value, the higher the operational performance attributable to alignment	0.713	Yes ($p < 0.05$)
H2: the higher the similarity value, the higher the overall performance attributable to alignment	0.404	Yes ($p < 0.05$)
H3: the higher the similarity value, the higher the value-based performance attributable to alignment	0.529	Yes ($p<0.05$)

4.4 High-level recommendation

A k-means-clustering analysis on the simulated SMSRL results has been performed (k=3). Based on its result shown in Table 5, a high-level recommendation can be made for each SMSRL cluster. The cells with bold-font values show the category of improvement a factory should focus on to have the largest impact on a respective performance category. For example, the first row indicates that improvements in the information connectivity (C4) is likely to have the best impact on the operational performance.

Table 6. High-level recommendation

SMSRL Centroid (mean score)	Performance Category	Standardized Coefficient of Independent Variables			
		C1	C2	C3	C4
Low (0.1957)	Financial	-0.0276	**0.1169**	-0.0035	-0.0048
	Operational	-0.0996	0.0511	-0.0471	**0.0753**
Med (0.4608)	Financial	**0.0179**	0.004	-0.0021	-0.0278
	Operational	-0.065	-0.0013	-0.1052	-0.0139
High (0.6453)	Financial	-0.0250	**0.0439**	-0.0074	-0.1083
	Operational	-0.0270	0.0327	-0.0109	**0.0672**

5 Conclusion and Remark

We introduced a new, smart manufacturing system readiness assessment (SMSRL). SMSRL measures the readiness using maturity scoring of four dimensions: Organizational, IT, Performance management, and Information connectivity maturities. The core of the smart manufacturing concept is the ability to use information effectively. The SMSRL assessment provides a quantitative measure of this ability. Such measure, which is in the form of an index, can be used for benchmarking. The statistical analysis shows that the index has a positive correlation with three types of performance: operational, overall, and value-based.

The SMSRL index provides a real number as its readiness measure. The SCRL, on the other hand, provides discrete readiness levels. Each type of measure has its advantages. Discrete measures lend themselves readily to definitional levels. Real-numbered levels do not; however, they can be used in other quantitative analysis – such as the ones shown in section 4. Discrete measures cannot

In our future work, we will 1) develop a method to provide more detailed improvement recommendations 2) extending and/or experimenting with other models used as a reference for the assessment.

Reference

1. Challenge Forecasting for Very Small Manufacturers, http://nistmep.blogs.govdelivery.com/challenge-forecasting-for-very-small-manufacturers/
2. Tucker, B. (2010). SCRL-model for Human Space Flight Operations enterprise supply chain.
3. MESA (2011). Transforming Manufacturing Maturity with ISA-95 Methods.

4. Mankins, J. C. (1995). Technology readiness levels. White Paper, April, 6.
5. Wheeler, D. J., & Ulsh, M. (2009). Manufacturing readiness assessment for fuel cell stacks and systems for the back-up power and material handling equipment emerging markets. National Renewable Energy Laboratory.
6. Jung, K., et al. “An Activity Model for Smart Factory Design and Improvement.”, Accepted to *Production Planning & Control*.
7. IEEE 1320.1 IEEE Functional Modeling Language – Syntax and Semantics for IDEF0, International Society of Electrical and Electronics Engineers, New York, 1998.
8. Jung, K., Doctoral Dissertation, Reference Activity Model-based Factory Design and Operations Evaluation Framework, Pohang University of Science and Technology
9. ANSI/ISA-88.00.01-2010 Batch Control Part 1: Models and Terminology
10. Raymond, L., & Paré, G. (1992). Measurement of information technology sophistication in small manufacturing businesses. Information Resources Management Journal (IRMJ), 5(2), 4-16.
11. Powell, D., et al. (2013). Lean production and ERP systems in small-and medium-sized enterprises: ERP support for pull production. Intl. J. of Production Research, 51(2), 395-409.
12. Maasouman, M. A., & Demirli, K. (2014). Development of a lean maturity model for operational level planning. Intl. J. of Advanced Manufacturing Technology, 1-18.
13. Chung, S. H., et al. (2003). The impact of information technology infrastructure flexibility on strategic alignment and application implementations. The Communications of the Association for Information Systems, 11(1), 44.
14. CMMI Product Team. (2010). CMMI for Development, Version 1.3.

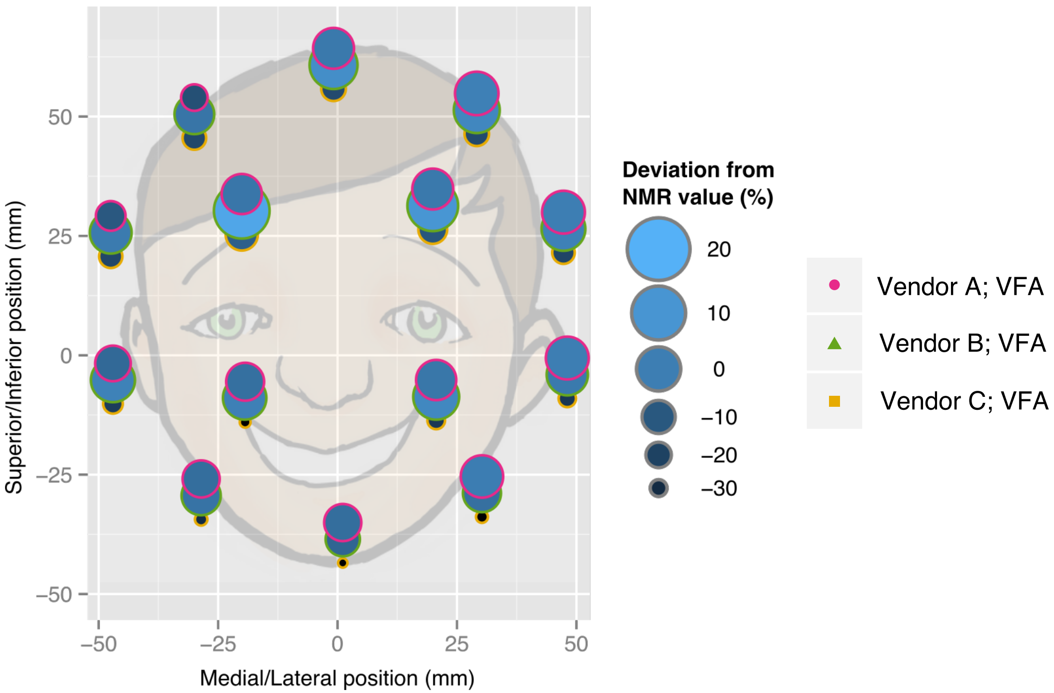
Tuesday, 11 AM

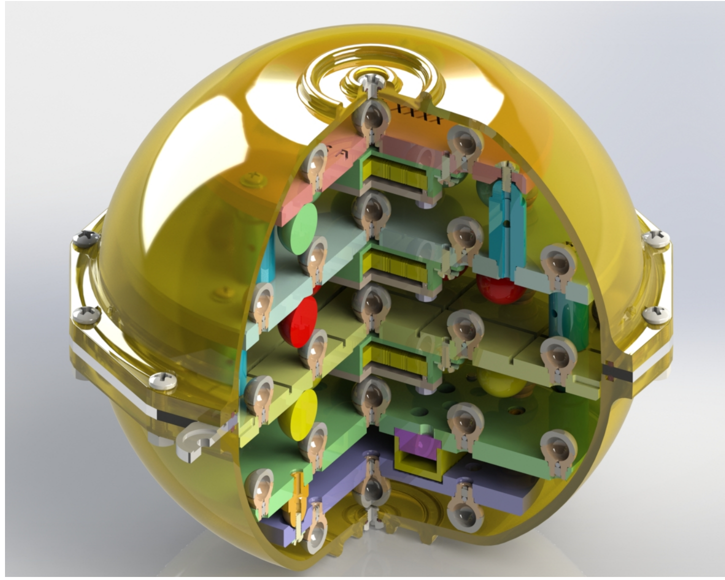
Computer #55

Program #3290

Comparison of T1 measurement using ISMRM/NIST phantom

Ad Hoc Committee on Standards for Quantitative MRI of the ISMRM





Tuesday, 11 AM

Computer #55

Program #3290

Multi-site, multi-vendor comparison of T1 measurement using ISMRM/NIST system phantom

Keenan KE[1], Stupic KF[1], Boss MA[1], Russek SE[1], Chenevert TL[2], Prasad PV[3], Reddick WE[4], Cecil KM[5], Zheng J[6], Hu P[7], Jackson EF[8], and the Ad Hoc Committee on Standards for Quantitative MRI[9]

[1]Physical Measurement Laboratory, National Institute of Standards and Technology, Boulder, CO; [2]University of Michigan, Ann Arbor, MI; [3]NorthShore University Health System, Evanston, IL; [4]St. Jude Children's Research Hospital, Memphis TN; [5]Cincinnati Children's Hospital Medical Center, Cincinnati, OH; [6]Washington University in St. Louis, St. Louis, MO; [7]University of California, Los Angeles, CA; [8]University of Wisconsin, Madison, WI; [9]International Society of Magnetic Resonance in Medicine

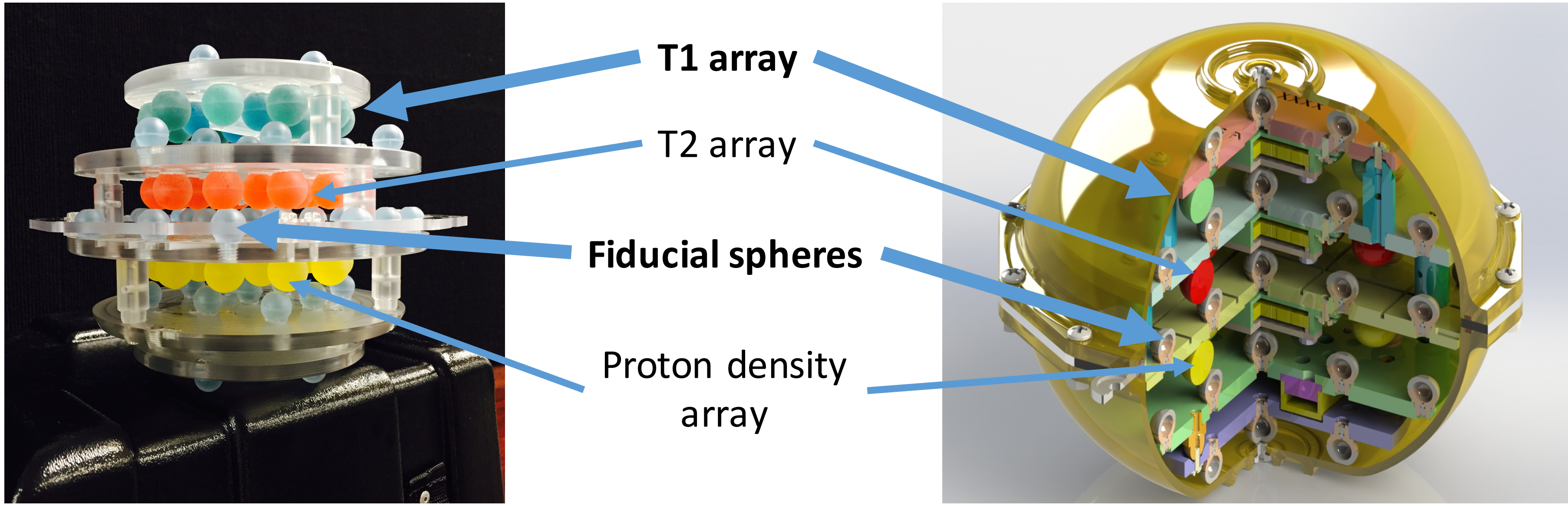
Multi-site, multi-vendor T1 measurement

- How does T1 measurement vary at one site day-to-day?
- How does T1 measurement vary across manufacturers?
- Is the variation different between 1.5 T and 3 T?
- Is the variation different between inversion recovery and variable flip angle methods?

ISMRM/NIST system phantom supports quantitative T1 and T2 measurements and can be used to answer these questions.

ISMRM/NIST System Phantom

- $NiCl_2$ solutions with varying concentrations for T1 range 20 to 2000 ms
- Reference T1 values measured on NMR by inversion recovery at 20 °C, 1.5 T and 3 T



T1 array

T2 array

Fiducial spheres

Proton density array

Photos courtesy of High Precision Devices.

Multi-site, multi-vendor Comparison

- Two system phantoms traveled the continental US
- Repeatability measurements (n=3) at one 3 T system for each manufacturer, coefficient of variation (CV)[1]
- Receive-only, head coils with 8 to 32 channels
- Reported temperature ranges: 17.1 to 23.3 °C

(of MRI room or bulk water in the phantom)

	1.5 T	3 T
Vendor A	1	3
Vendor B	1	3
Vendor C	5	5

[1] Sullivan DC, Obuchowski NA, Kessler LG, et al. Metrology Standards for Quantitative Imaging Biomarkers. Radiology. 2015

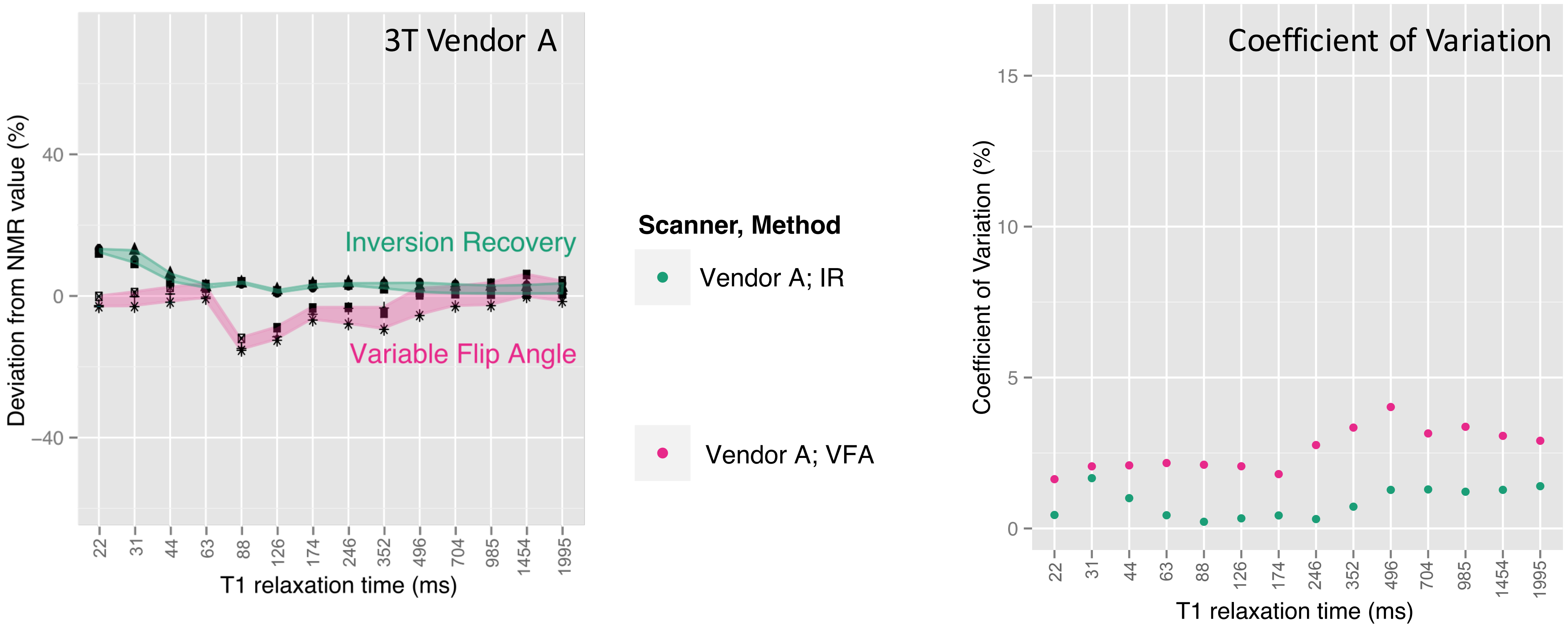
T1 Measurement Protocol

Inversion Recovery	
Sequence	Fast, SE-IR, 2D
Scan Plane	Coronal
Thickness (mm)	6
TR (ms)	4500
TE (ms)	~ 7 (minimum full)
Inversion Times (ms)	35*, 50, 75, 100, 125, 150, 250, 1000, 1500, 2000, 3000
Averages	1
Echo Train Length	6
Pixel Size (mm x mm)	0.98 x 0.98
Note: TI = 35 ms not available on Vendor A.	

Variable Flip Angle	
Sequence	Fast, SPGR, 3D
Scan Plane	Coronal
Thickness (mm)	3 (no gap)
TR (ms)	~ 6.6
TE (ms)	Minimum: 1.5-2.5
Flip Angles	2, 5, 10, 15, 20, 25, 30
Averages	4
Echo Train Length	1
Pixel Size (mm x mm)	0.98 x 0.98
Note: Prescan on FA=15°, no subsequent gain changes.	

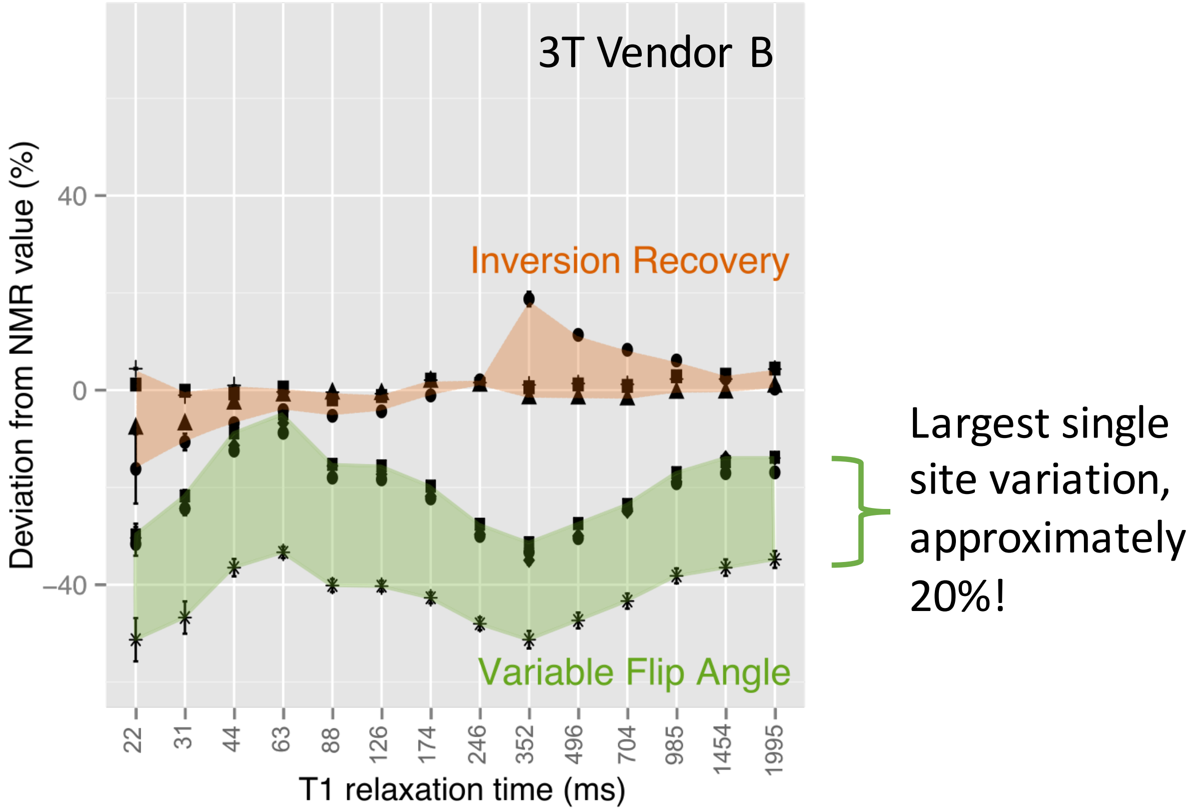
- Data fit using custom software (PhantomViewer, developed at NIST)

Vendor A, 3T, repeatability measurements

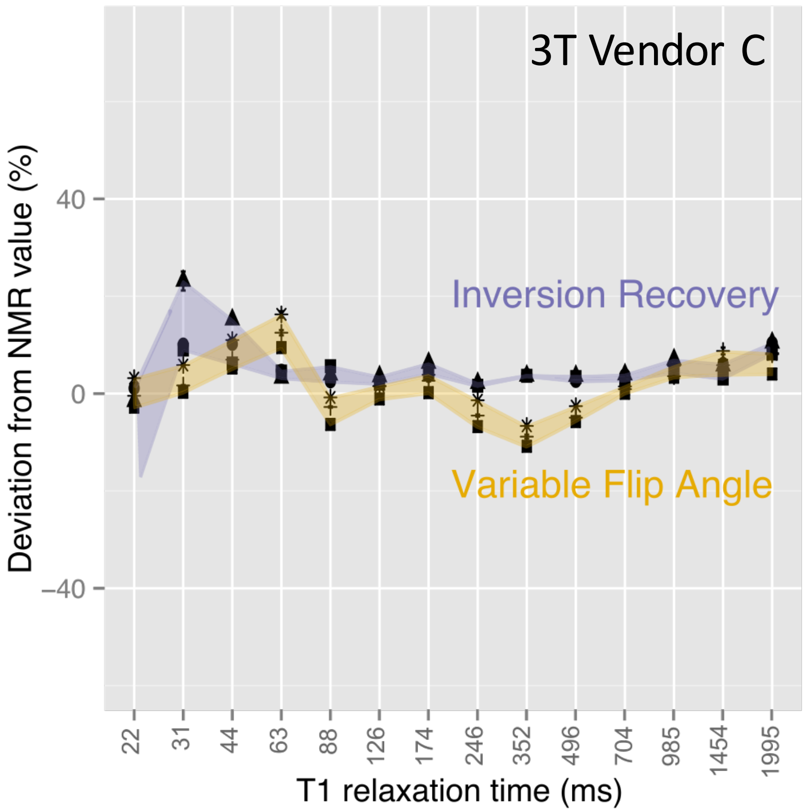


Colored bands show the range of values at a single repeatability site.

Vendors B and C, 3T, repeatability measurements

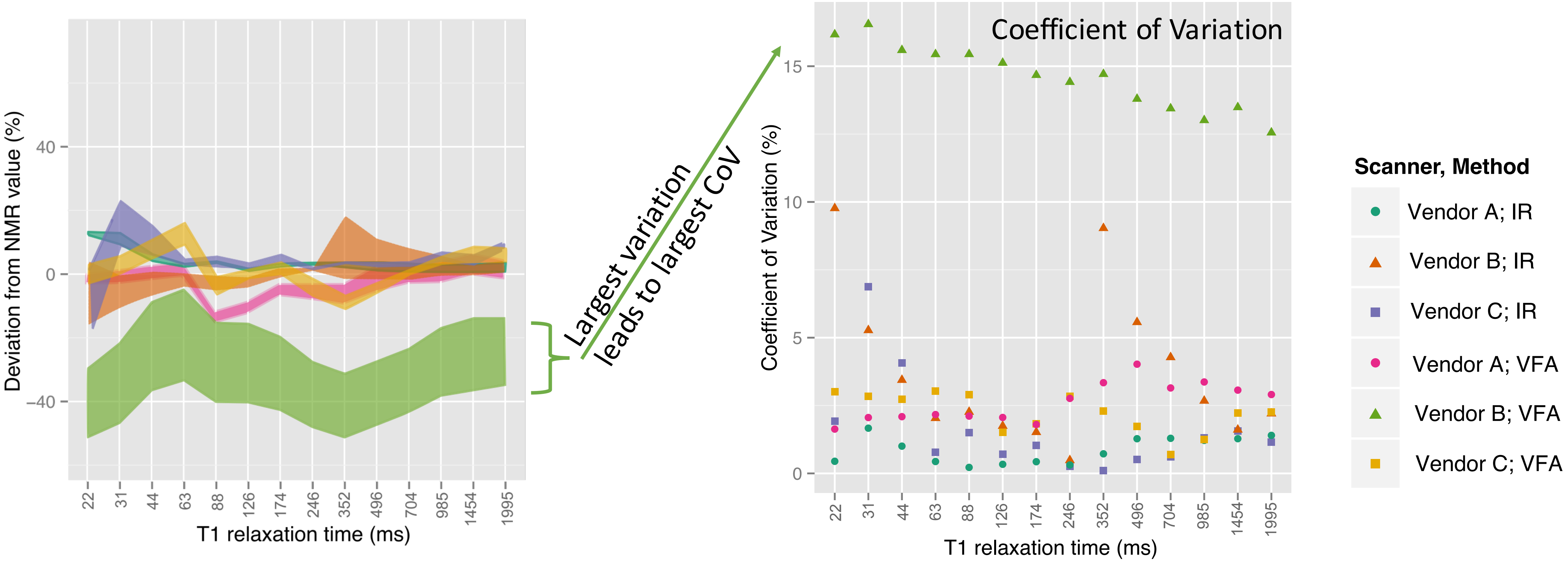


Largest single site variation, approximately 20%!



Colored bands show the range of values at a single repeatability site.

All repeatability measurements at 3 T

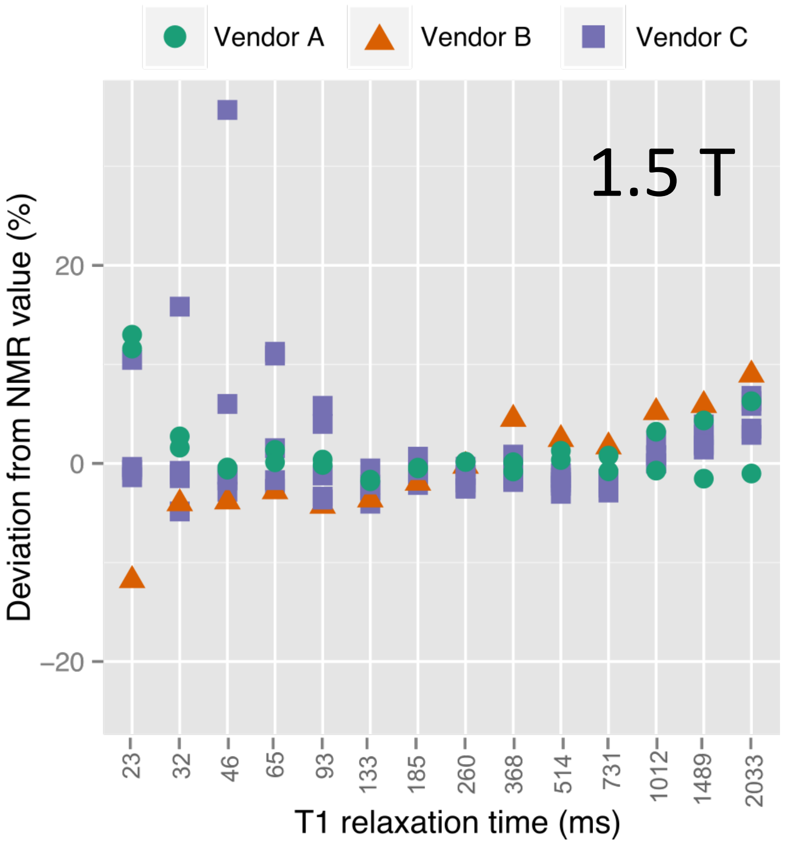


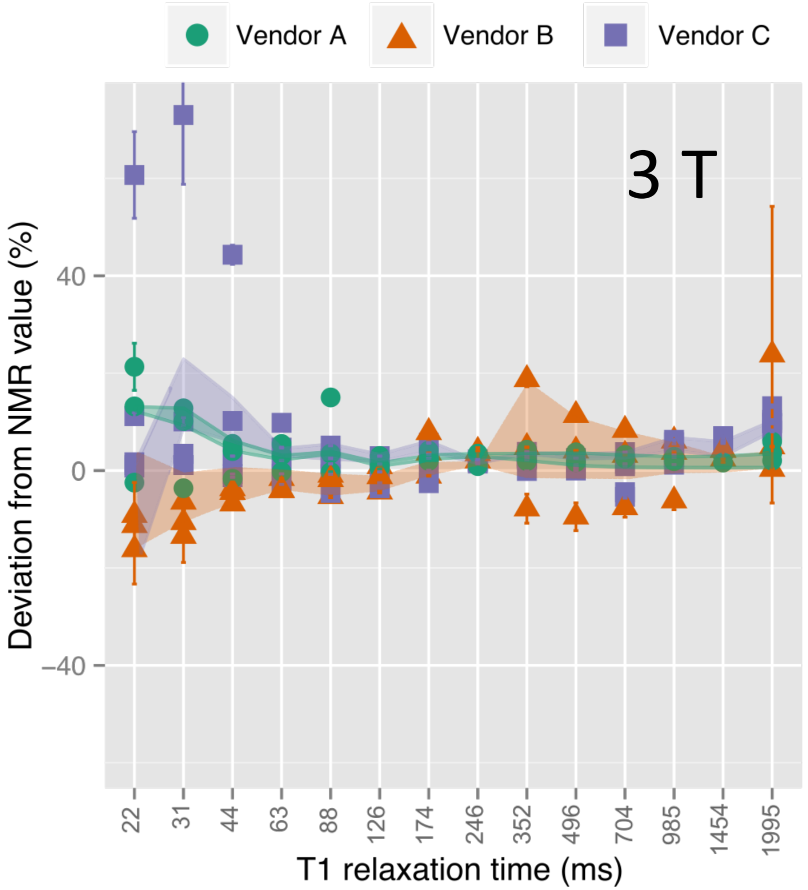
Largest variation leads to largest CoV

Coefficient of Variation

Colored bands show the range of values at a single repeatability site.

Inversion Recovery: MRI comparison to NMR measured values





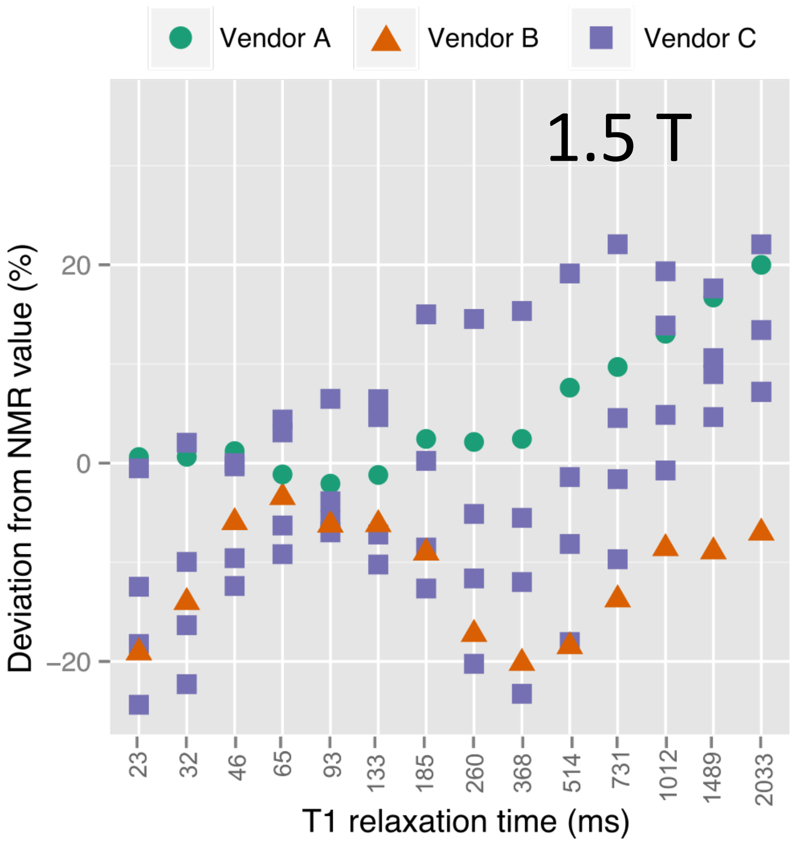
Note: 3 T y-axis range is 2x the 1.5 T y-axis range.

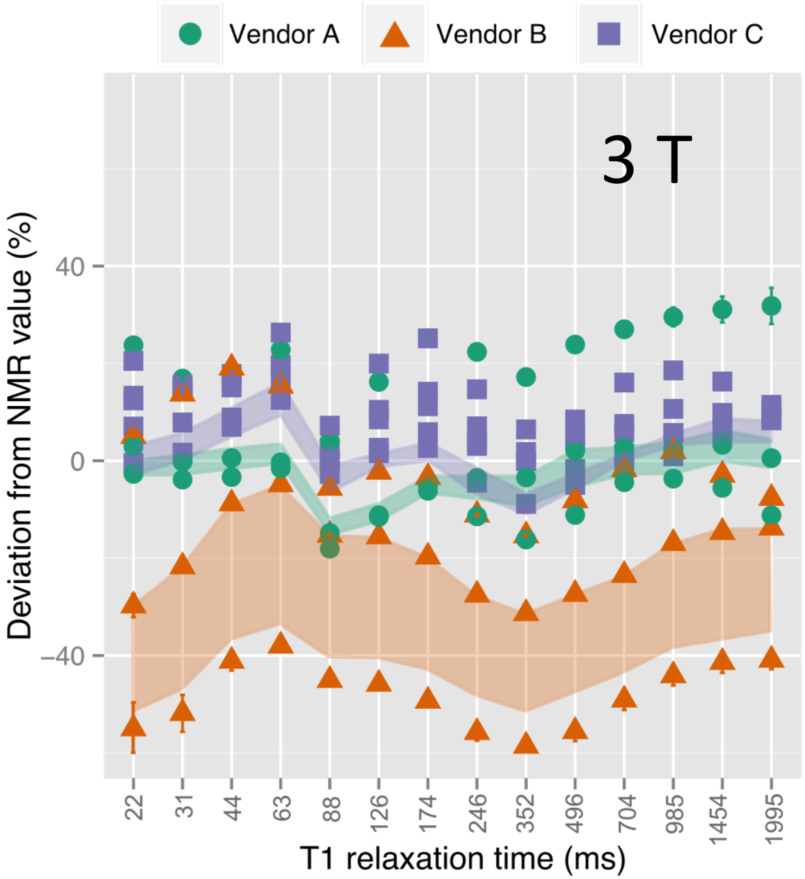
Colored bands show the range of values at a single repeatability site.

Overall, Inversion Recovery is accurate.

Difficulty fitting short T1 times likely due to selected inversion times.

Variable Flip Angle: MRI comparison to NMR measured values



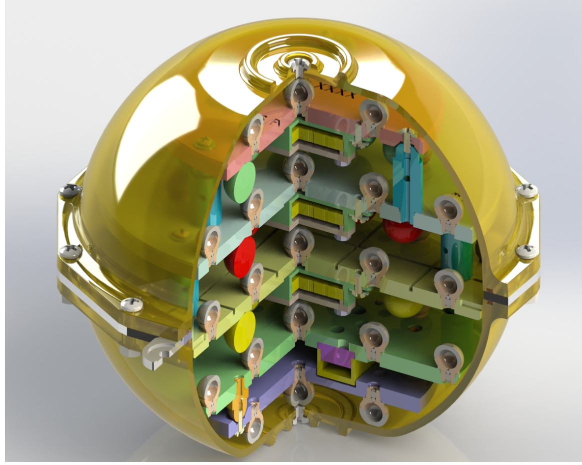


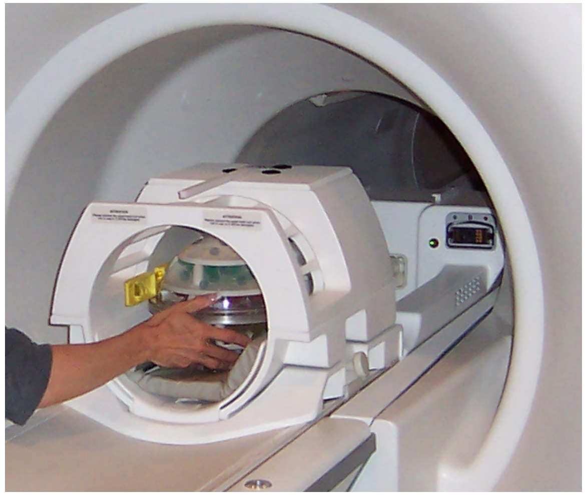
Note: 3 T y-axis range is 2x the 1.5 T y-axis range.

Colored bands show the range of values at a single repeatability site.

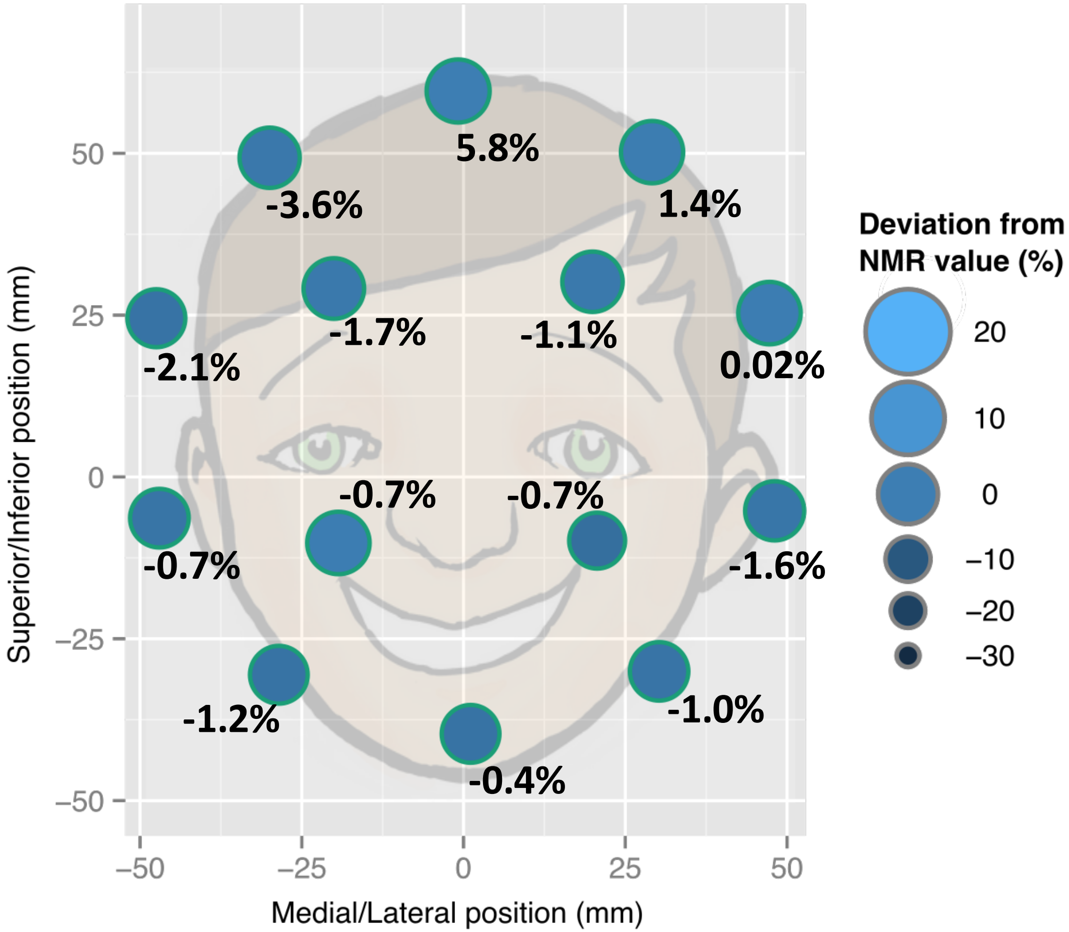
Can we understand the systematic patterns in the 3 T data?

Spatial dependence of variations: Inversion Recovery



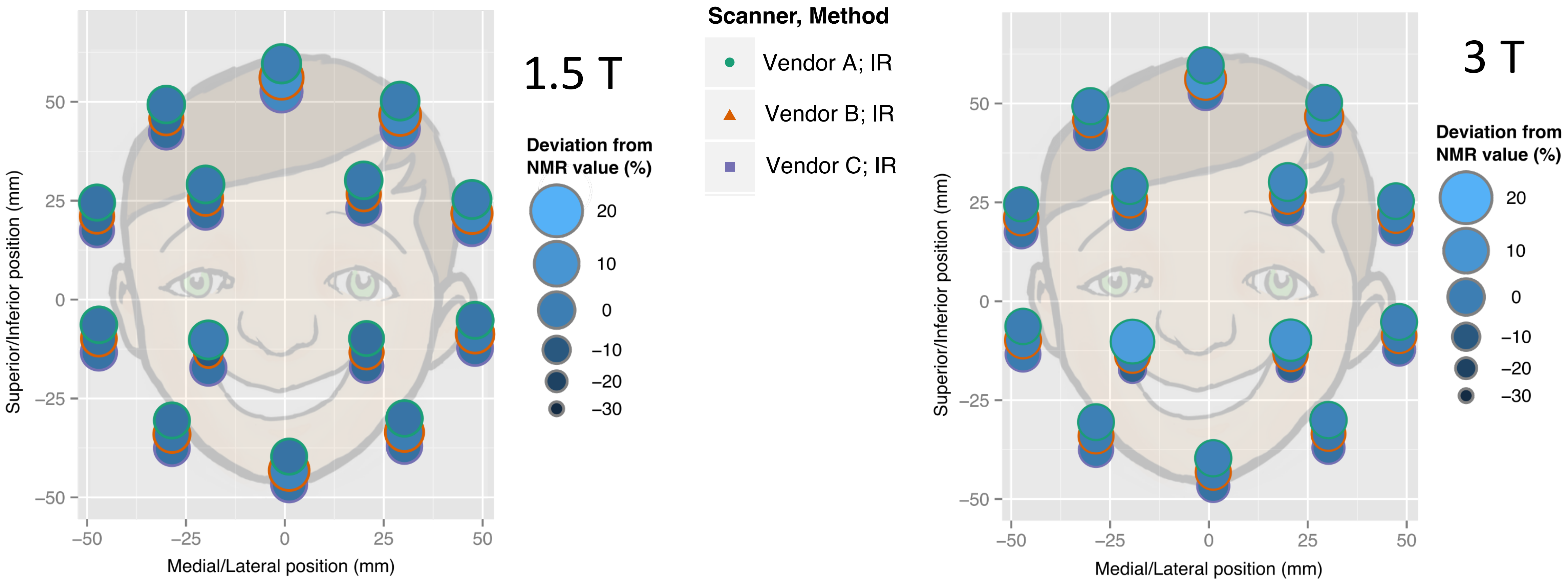


Inversion Recovery, 1.5 T data from Vendor A



Deviation from NMR values ranges from -3.6 to 5.8 %

Spatial dependence of variations: Inversion Recovery



Vendor A deviation: -3.6 to 5.8 %

Vendor B deviation: -11.8 to 8.9 %

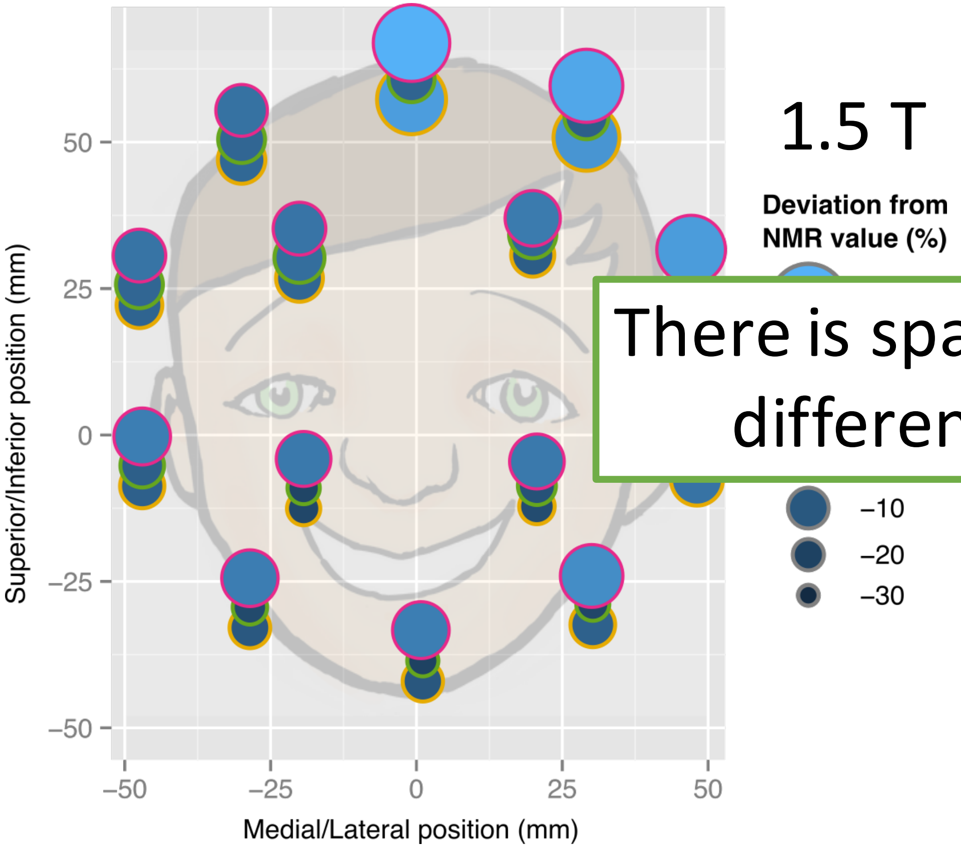
Vendor C deviation: -4.8 to 6.3 %

Vendor A deviation: 0.9 to 13.2 %

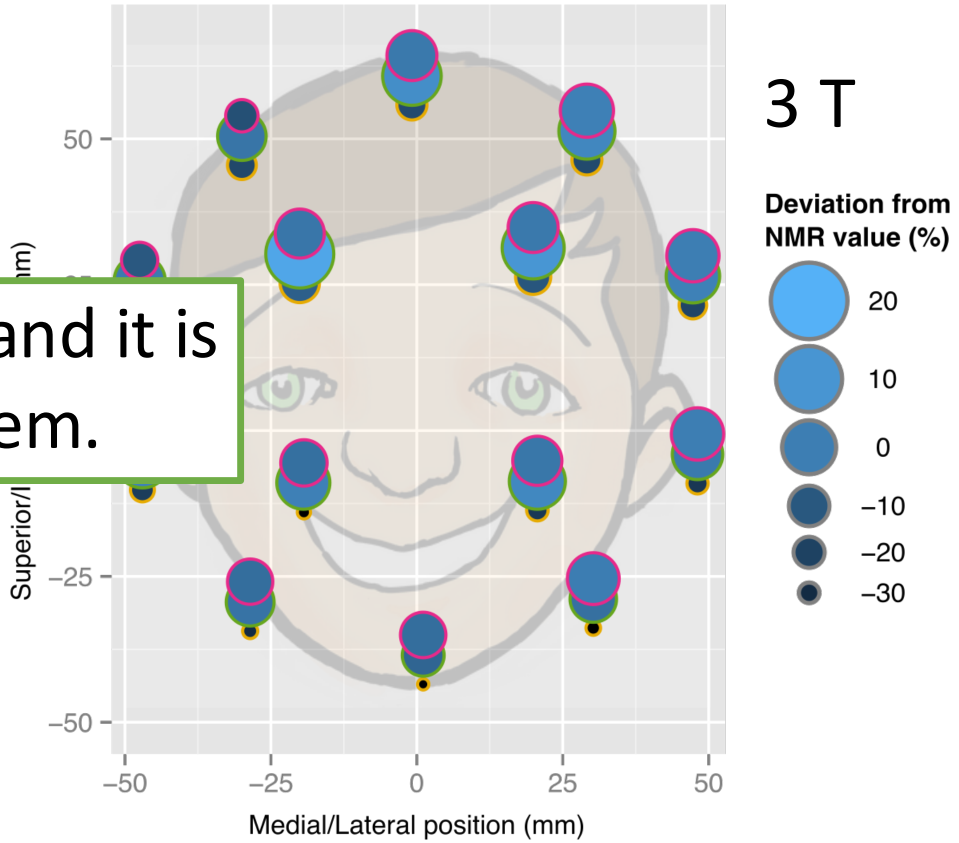
Vendor B deviation: -8.0 to 1.7 %

Vendor C deviation: 0.4 to 9.7 %

Spatial dependence of variations: Variable Flip Angle



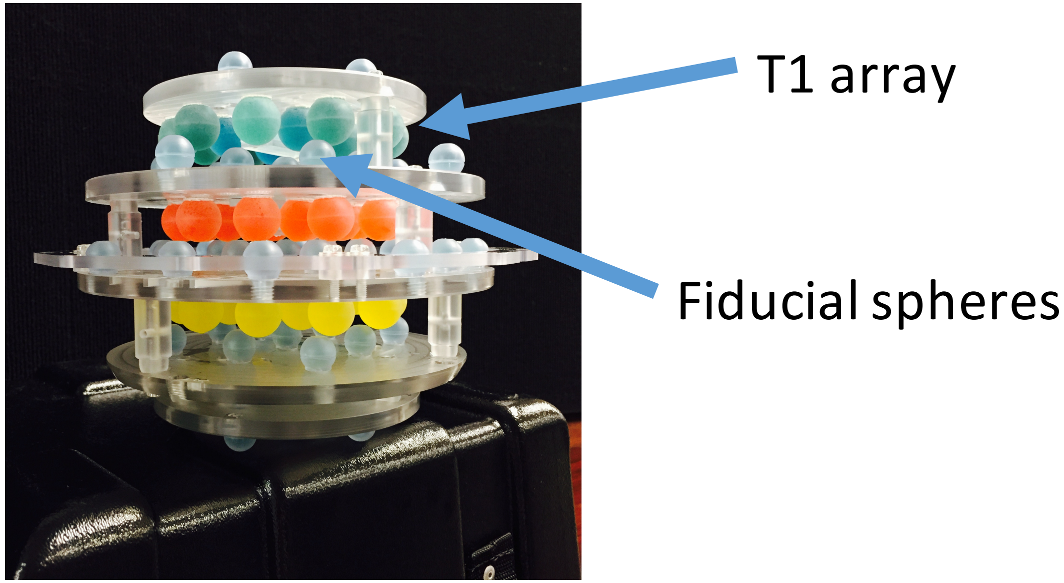
There is spatial variation, and it is different for each system.



Vendor A deviation: -2.1 to 20.0 %
Vendor B deviation: -20.2 to -3.4 %
Vendor C deviation: -18.2 to 13.4 %

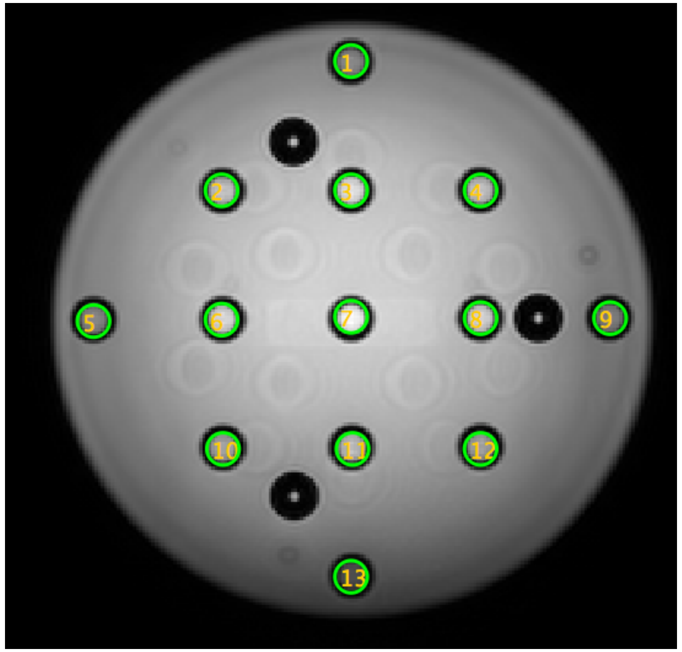
Vendor A deviation: -14.8 to 3.3 %
Vendor B deviation: -33.3 to -8.8 %
Vendor C deviation: -6.6 to 16.3 %

Spatial dependence of variations: **Fiducial Sphere Plane**



T1 array

Fiducial spheres

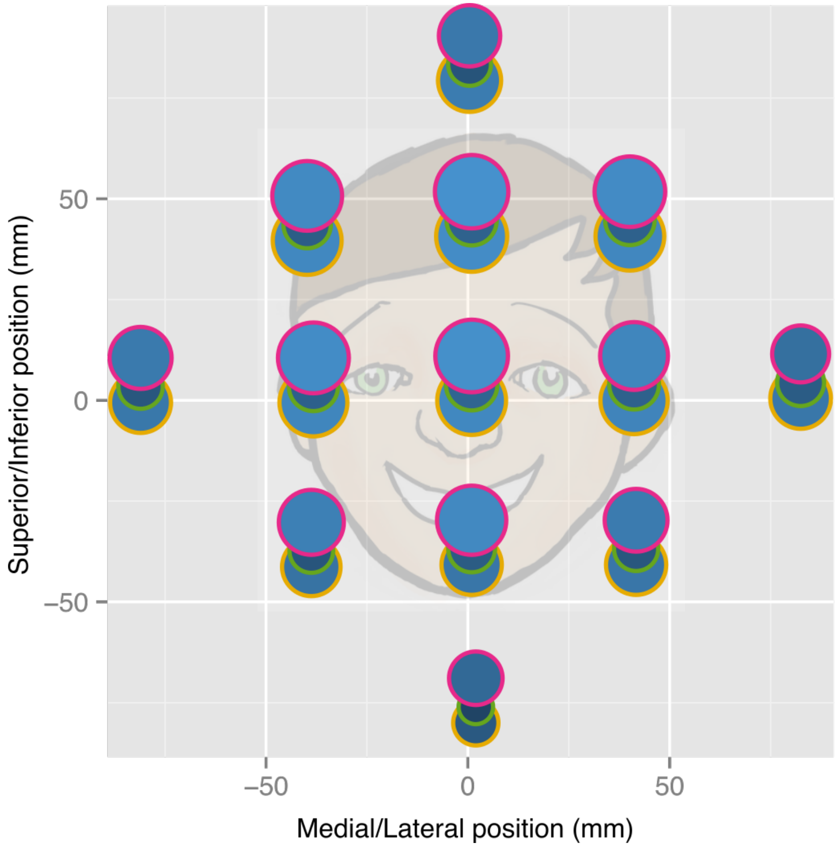


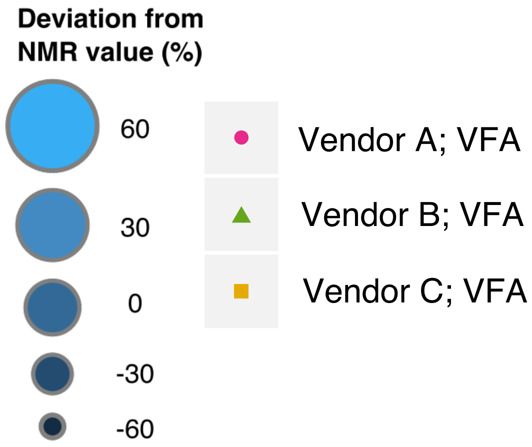
Fiducial spheres are located below the T1 array, within the 3D VFA imaging section.

Fiducial spheres all contain the same concentration of $CuSO_4$.

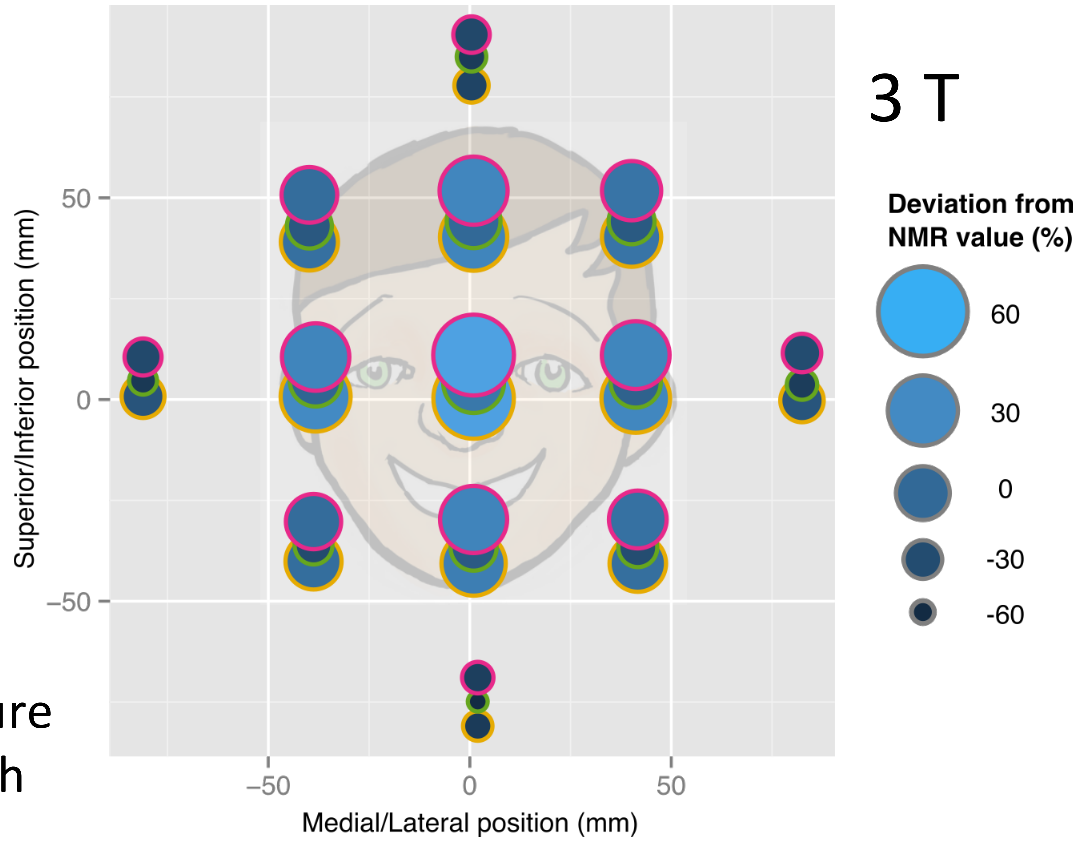
Spatial dependence of variations: Variable Flip Angle

1.5 T





3 T



$CuSO_4$ is more temperature sensitive than $NiCl_2$, which affects our ability to interpret these results.

Vendor A deviation: -0.7 to 37.3 %

Vendor B deviation: -37.1 to -4.7 %

Vendor C deviation: -16.6 to 32.4 %

Vendor A deviation: -42.9 to 51.2 %

Vendor B deviation: -65.0 to -13.2 %

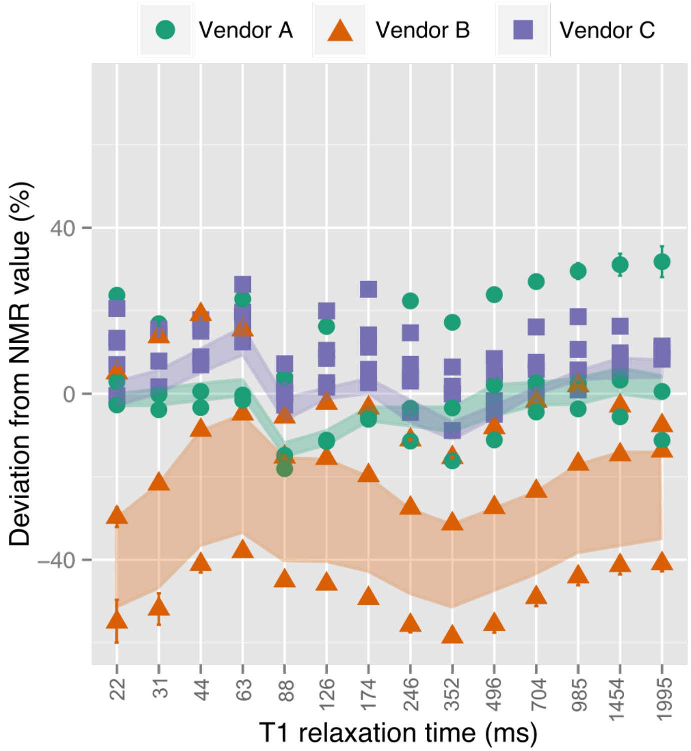
Vendor C deviation: -46.7 to 50.7 %

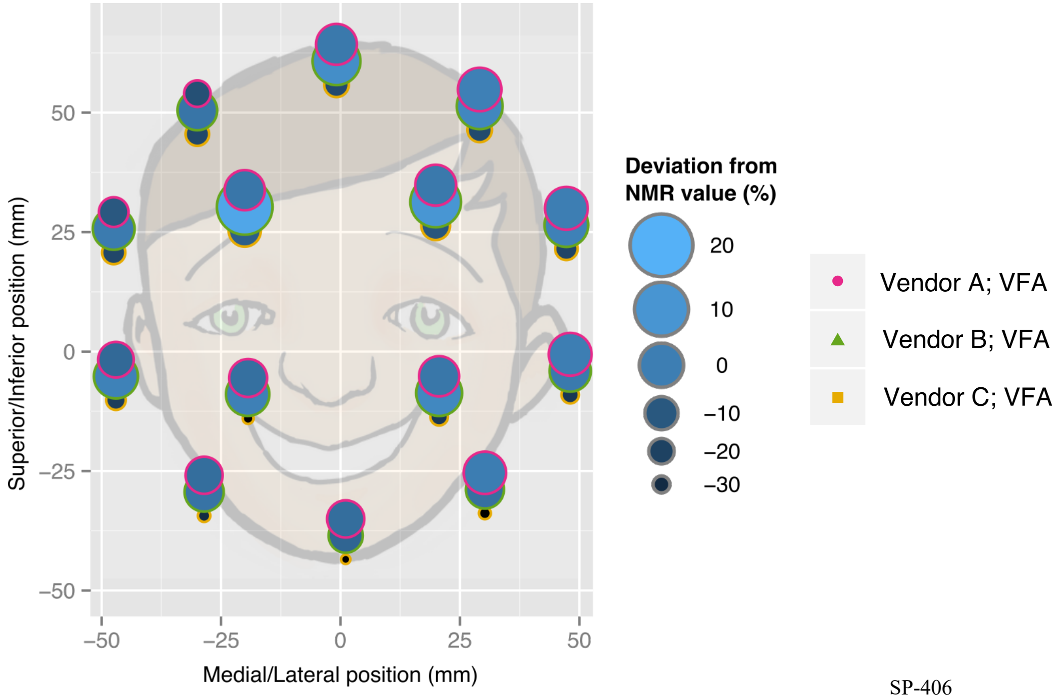
Why the deviation from known values?

- NMR methods v. MRI methods
- Temperature sensitivity over the reported temperatures
    - Non-linear, increases by 7.2% over the range of reported temperatures
    - *Deviation from reference T1 cannot be attributed only to temperature*
- Best efforts for similar protocol, but B1 pulse profiles unknown and could change across range of flip angles
- NMR deviation patterns suggest possible B1 effect

Multi-site, multi-vendor T1 variation

- T1 variations from NMR-measured value are correlated site-to-site within a vendor and by position within the head coil
- ISMRM/NIST system phantom is an excellent tool for evaluation multi-site acquisition protocols





Acknowledgments

- We appreciate the efforts of all those who completed the scans of the phantom, especially when we asked them to repeat their efforts.

- We thank the SQMR committee past and present. Current members of the SQMR committee are:

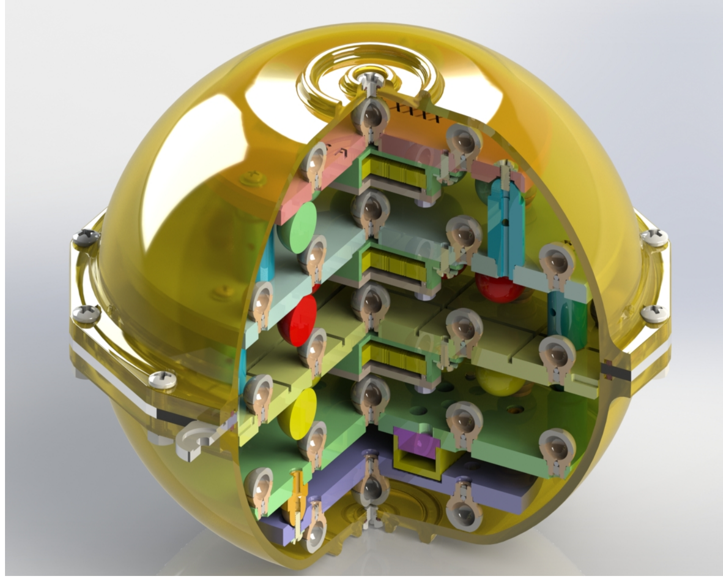
Michael A. Boss
Jeff L. Gunter
Kim Maria Cecil
Thomas L. Chenevert
Daniel Gembris
Alexander S. R. Guimaraes
Peng Hu
Xiaoping P. Hu
Clifford R. Jack
Edward F. Jackson
Kathryn E. Keenan
Pottumarthi Vara Prasad
Wilburn E. Reddick
Stephen E. Russek
Michael Salerno
Amita Shukla-Dave
Michael Steckner
Karl F. Stupic
Chung Yuan
Huiming Zhang
Jie Zheng

For more information on NIST phantoms in development, the NIST/ISMRM phantom and to provide input, please visit:

http://collaborate.nist.gov/mriphantoms

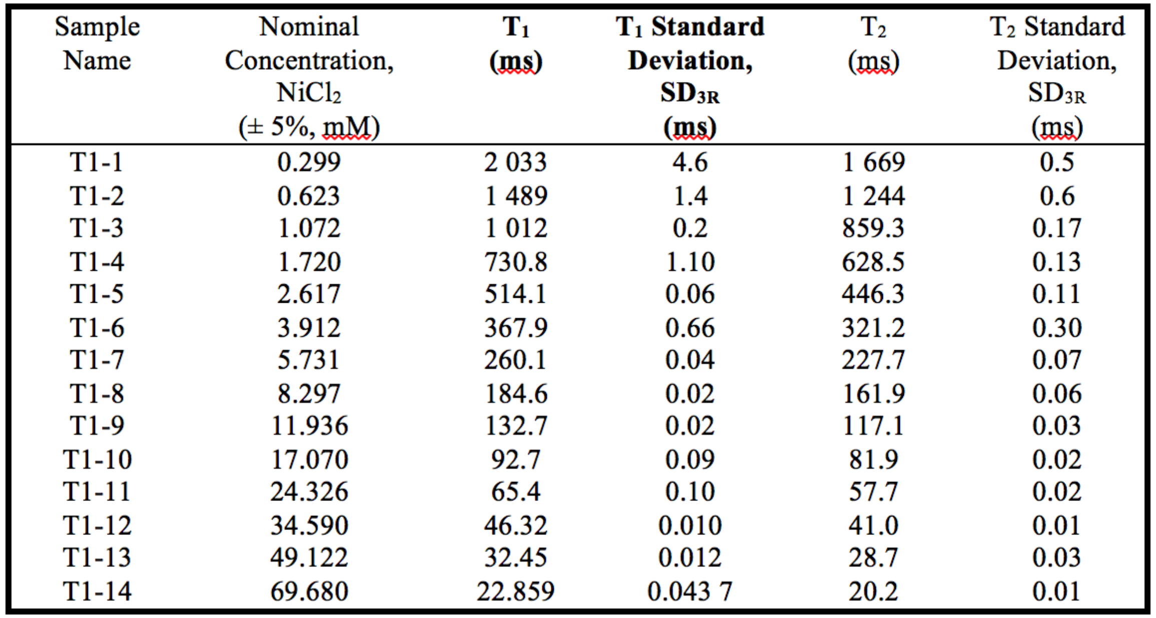
To contact the author:

kathryn [dot] keenan [at] nist [dot] gov



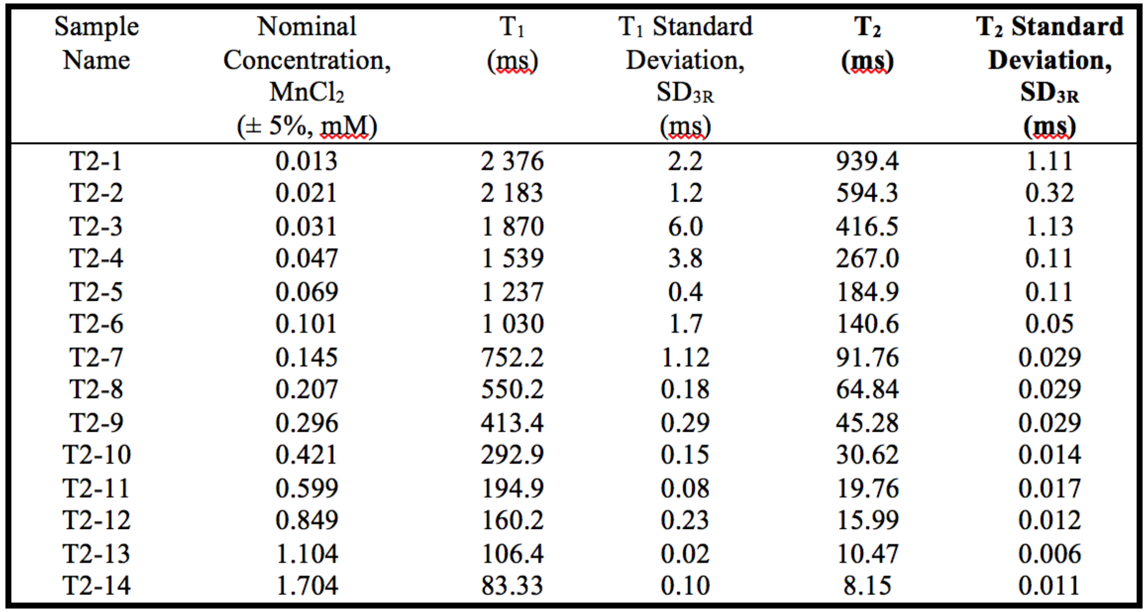
Reference Measurements: 1.5 T NMR

T1 array



Sample Name	Nominal Concentration, $NiCl_2$ (± 5%, mM)	**T_1 (ms)**	**T_1 Standard Deviation, SD_{3R} (ms)**	T_2 (ms)	T_2 Standard Deviation, SD_{3R} (ms)
T1-1	0.299	2 033	4.6	1 669	0.5
T1-2	0.623	1 489	1.4	1 244	0.6
T1-3	1.072	1 012	0.2	859.3	0.17
T1-4	1.720	730.8	1.10	628.5	0.13
T1-5	2.617	514.1	0.06	446.3	0.11
T1-6	3.912	367.9	0.66	321.2	0.30
T1-7	5.731	260.1	0.04	227.7	0.07
T1-8	8.297	184.6	0.02	161.9	0.06
T1-9	11.936	132.7	0.02	117.1	0.03
T1-10	17.070	92.7	0.09	81.9	0.02
T1-11	24.326	65.4	0.10	57.7	0.02
T1-12	34.590	46.32	0.010	41.0	0.01
T1-13	49.122	32.45	0.012	28.7	0.03
T1-14	69.680	22.859	0.043 7	20.2	0.01

T2 array



Sample Name	Nominal Concentration, $MnCl_2$ (± 5%, mM)	T_1 (ms)	T_1 Standard Deviation, SD_{3R} (ms)	**T_2 (ms)**	**T_2 Standard Deviation, SD_{3R} (ms)**
T2-1	0.013	2 376	2.2	939.4	1.11
T2-2	0.021	2 183	1.2	594.3	0.32
T2-3	0.031	1 870	6.0	416.5	1.13
T2-4	0.047	1 539	3.8	267.0	0.11
T2-5	0.069	1 237	0.4	184.9	0.11
T2-6	0.101	1 030	1.7	140.6	0.05
T2-7	0.145	752.2	1.12	91.76	0.029
T2-8	0.207	550.2	0.18	64.84	0.029
T2-9	0.296	413.4	0.29	45.28	0.029
T2-10	0.421	292.9	0.15	30.62	0.014
T2-11	0.599	194.9	0.08	19.76	0.017
T2-12	0.849	160.2	0.23	15.99	0.012
T2-13	1.104	106.4	0.02	10.47	0.006
T2-14	1.704	83.33	0.10	8.15	0.011

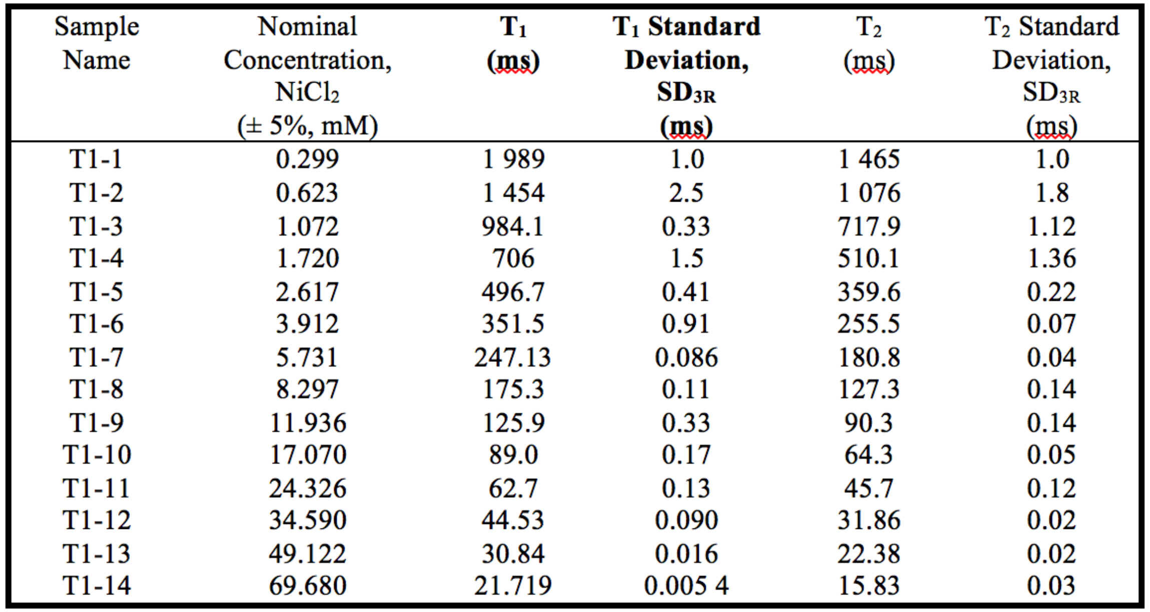
Aliquots of each solution were sealed into 2 mm outside diameter (OD) quartz ($NiCl_2$ solutions) or 3 mm (OD) PTFE ($MnCl_2$ solutions) NMR tubes. Quartz samples were sealed using a methane/oxygen torch to flame seal. PTFE samplers were sealed with a PTFE plug inserted 1 cm into the sample tube. A fiber optic temperature probe was positioned with the sensor in the middle of the radiofrequency (RF) coil. Each sample was equilibrated to 293.00 K (conditions noted below) for a minimum of 15 minutes. Samples were shimmed using the Berger-Braun shimming method prior to collecting relaxation time data.

NMR details of NMR-IR experiments can be found in: *200 and More NMR Experiments: A Practical Course, S. Berger & S. Braun*, ISBN-13: 978-3527310678.

NMR details of NMR-CPMG experiments can be found in: *200 and More NMR Experiments: A Practical Course, S. Berger & S. Braun*, ISBN-13: 978-3527310678.

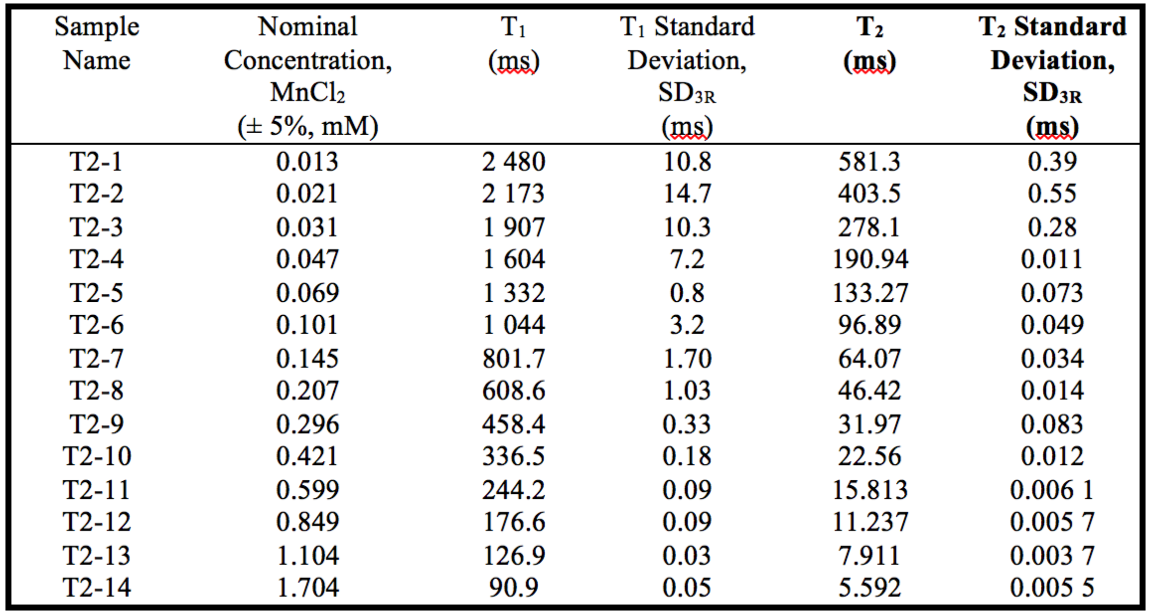
Reference Measurements: 3 T NMR

T1 array



Sample Name	Nominal Concentration, $NiCl_2$ (± 5%, mM)	**T_1 (ms)**	**T_1 Standard Deviation, SD_{3R} (ms)**	T_2 (ms)	T_2 Standard Deviation, SD_{3R} (ms)
T1-1	0.299	1 989	1.0	1 465	1.0
T1-2	0.623	1 454	2.5	1 076	1.8
T1-3	1.072	984.1	0.33	717.9	1.12
T1-4	1.720	706	1.5	510.1	1.36
T1-5	2.617	496.7	0.41	359.6	0.22
T1-6	3.912	351.5	0.91	255.5	0.07
T1-7	5.731	247.13	0.086	180.8	0.04
T1-8	8.297	175.3	0.11	127.3	0.14
T1-9	11.936	125.9	0.33	90.3	0.14
T1-10	17.070	89.0	0.17	64.3	0.05
T1-11	24.326	62.7	0.13	45.7	0.12
T1-12	34.590	44.53	0.090	31.86	0.02
T1-13	49.122	30.84	0.016	22.38	0.02
T1-14	69.680	21.719	0.005 4	15.83	0.03

T2 array



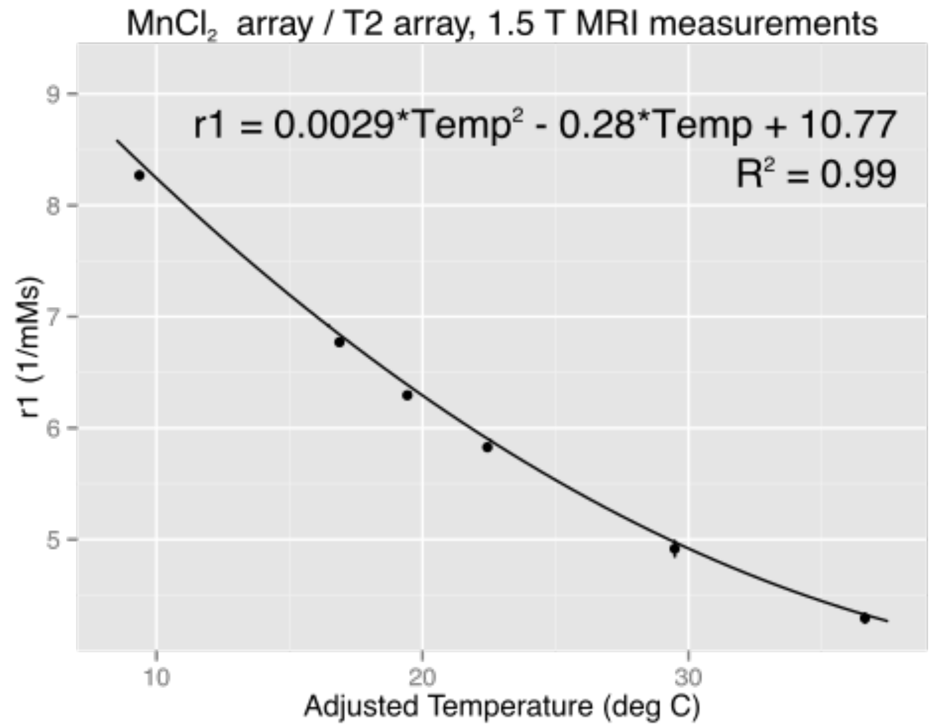
Sample Name	Nominal Concentration, $MnCl_2$ (± 5%, mM)	T_1 (ms)	T_1 Standard Deviation, SD_{3R} (ms)	**T_2 (ms)**	**T_2 Standard Deviation, SD_{3R} (ms)**
T2-1	0.013	2 480	10.8	581.3	0.39
T2-2	0.021	2 173	14.7	403.5	0.55
T2-3	0.031	1 907	10.3	278.1	0.28
T2-4	0.047	1 604	7.2	190.94	0.011
T2-5	0.069	1 332	0.8	133.27	0.073
T2-6	0.101	1 044	3.2	96.89	0.049
T2-7	0.145	801.7	1.70	64.07	0.034
T2-8	0.207	608.6	1.03	46.42	0.014
T2-9	0.296	458.4	0.33	31.97	0.083
T2-10	0.421	336.5	0.18	22.56	0.012
T2-11	0.599	244.2	0.09	15.813	0.006 1
T2-12	0.849	176.6	0.09	11.237	0.005 7
T2-13	1.104	126.9	0.03	7.911	0.003 7
T2-14	1.704	90.9	0.05	5.592	0.005 5

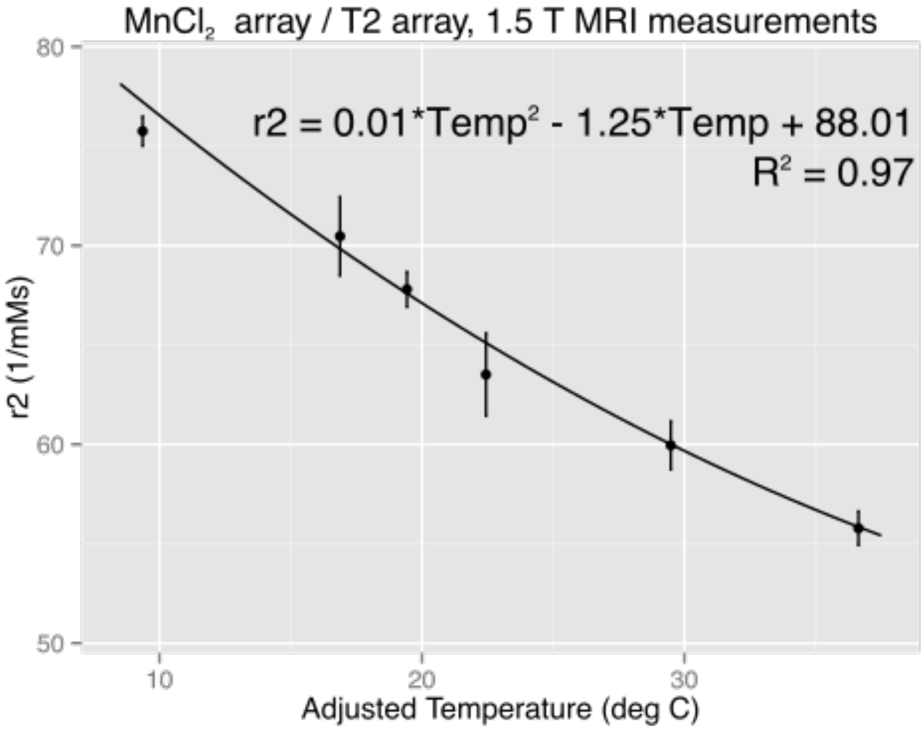
Aliquots of each solution were sealed into 2 mm outside diameter (OD) quartz ($NiCl_2$ solutions) or 3 mm (OD) PTFE ($MnCl_2$ solutions) NMR tubes. Quartz samples were sealed using a methane/oxygen torch to flame seal. PTFE samplers were sealed with a PTFE plug inserted 1 cm into the sample tube. A fiber optic temperature probe was positioned with the sensor in the middle of the radiofrequency (RF) coil. Each sample was equilibrated to 293.00 K (conditions noted below) for a minimum of 15 minutes. Samples were shimmed using the Berger-Braun shimming method prior to collecting relaxation time data.

NMR details of NMR-IR experiments can be found in: *200 and More NMR Experiments: A Practical Course, S. Berger & S. Braun*, ISBN-13: 978-3527310678.

NMR details of NMR-CPMG experiments can be found in: *200 and More NMR Experiments: A Practical Course, S. Berger & S. Braun*, ISBN-13: 978-3527310678.

Reference Measurements: temperature dependence





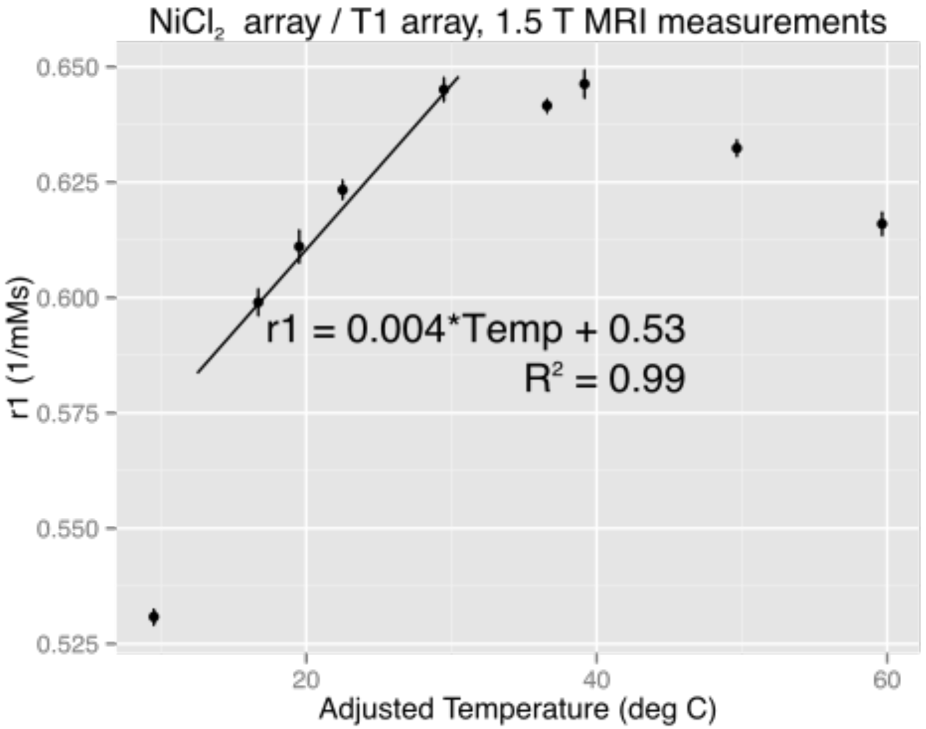
Preliminary assessment of temperature dependence

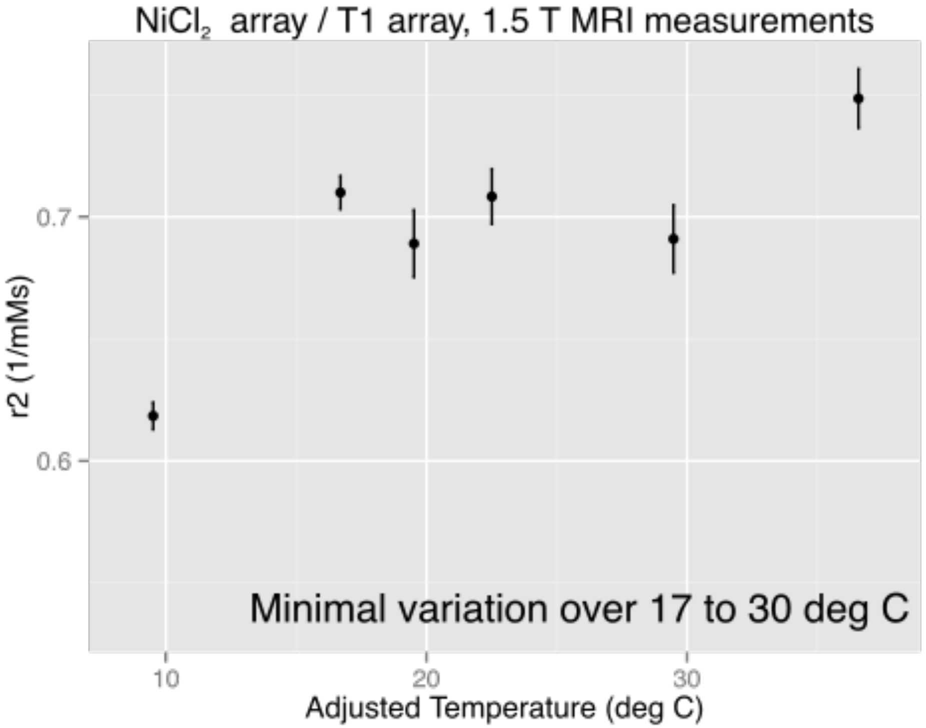
Sample spheres, the same as those used in the commercial phantoms, were imaged on a 1.5 T small-bore system. A temperature-control system was used with a fiber-optic probe to achieve temperatures of approximately 10, 17, 20, 23, 30 and 37 °C.

Inversion recovery spin-echo was used to measure T1 relaxation time with: TR = 10 s, TE = 20 ms, TI = 50, 75, 100, 125, 150, 250, 500, 1000, 1500, 2000 and 3000 ms.

Spin echo was used to measure T2 relaxation time with: TR = 10 s, TE = 15, 20, 40, 80, 160, and 320 ms.

Reference Measurements: temperature dependence





Preliminary assessment of temperature dependence
Sample spheres, the same as those used in the commercial phantoms, were imaged on a 1.5 T small-bore system. A temperature-control system was used with a fiber-optic probe to achieve temperatures of approximately 10, 17, 20, 23, 30 and 37 °C.
Inversion recovery spin-echo was used to measure T1 relaxation time with: TR = 10 s, TE = 20 ms, TI = 50, 75, 100, 125, 150, 250, 500, 1000, 1500, 2000 and 3000 ms.
Spin echo was used to measure T2 relaxation time with: TR = 10 s, TE = 15, 20, 40, 80, 160, and 320 ms.

Evaluating the Oxidative Potential of Indoor and Outdoor Particles with an EPR Assay

Shahana Khurshid
Steven J. Emmerich
Andrew Persily

Engineering Laboratory, National Institute of Standards and Technology
100 Bureau Drive Gaithersburg, MD 20899

Content submitted to and published by:
14th International Conference on Indoor Air Quality
and Climate, Ghent, BE
July 3rd – July 8th, 2016

U.S. Department of Commerce
Penny Pritzker, Secretary of Commerce

National Institute of Standards and Technology
Willie E May, Director

NIST National Institute of Standards and Technology • U.S. Department of Commerce

SP-413

Khurshid, Shahana; Emmerich, Steven; Persily, Andrew.
"Evaluating the Oxidative Potential of Indoor and Outdoor Particles with an EPR Assay."
Paper presented at the International Conference on Indoor Air Quality and Climate Conference, Ghent, Belgium, Jul 3-Jul 8, 2016.

DISCLAIMERS

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Any link(s) to website(s) in this document have been provided because they may have information of interest to our readers. NIST does not necessarily endorse the views expressed or the facts presented on these sites. Further, NIST does not endorse any commercial products that may be advertised or available on these sites.

Khurshid, Shahana; Emmerich, Steven; Persily, Andrew.
"Evaluating the Oxidative Potential of Indoor and Outdoor Particles with an EPR Assay."
Paper presented at the International Conference on Indoor Air Quality and Climate Conference, Ghent, Belgium, Jul 3-Jul 8, 2016.

Evaluating the Oxidative Potential of Indoor and Outdoor Particles with an EPR Assay

Shahana S. Khurshid[1,*], Steven Emmerich [1], Andrew Persily[1]

[1]Energy and Environment Division, Engineering Laboratory, 100 Bureau Drive, Mail Stop 8633, Gaithersburg, MD 20899-8633, USA

[*]*Corresponding email: shahana.khurshid@nist.gov*

SUMMARY

The hydroxyl radical (•OH) generating capacity of particles has been measured in several outdoor locations, but it remains unquantified in indoor environments where extended periods of human exposure are likely. Total suspended particle samples were collected inside and outside an unoccupied manufactured test house in Maryland, USA. The oxidative potential of particles was determined using electron paramagnetic resonance (OP^{EPR}) to quantify the •OH produced when particles are placed in a hydrogen peroxide solution. The mean OP^{EPR} of indoor particles was about 75 % of the mean OP^{EPR} of outdoor particles on an air sampling volume basis. Given that particle counts were lower indoors than outdoors, the ratio of indoor to outdoor particulate OP^{EPR} is bound to be higher on a particle mass basis. Air change rate, temperature, and relative humidity were concurrently measured in order to assess the role of these parameters on the oxidative potential of particles.

PRACTICAL IMPLICATIONS

The free radical generating capacity of particles may provide a more relevant health-based exposure measure for particles as compared to particle size and concentration. This study quantifies the hydroxyl radical (•OH) generating capacity of particles collected in a test house under different conditions.

KEYWORDS

Particulate matter, Hydroxyl radical, Test house, Oxidative stress, Health effects

1 INTRODUCTION

It is widely accepted that airborne particles have adverse effects on human health but the pathophysiological mechanisms for these effects haven't been established (Bell et al., 2004, Pope et al., 2015). Particulate matter (PM) are typically characterized by their physical properties and chemical composition, but there may be more physiologically relevant properties of PM that are better suited to characterize their ability to induce cellular oxidative stress (Borm et al., 2007). The hydroxyl radical (•OH) generating capacity of PM has been suggested as a way to assess the oxidative potential of particles (Shi et al., 2003b). Transition metals are known to drive •OH generation via the Fenton reaction, which involves the reduction of hydrogen peroxide (H_2O_2) by a transition metal (Shi et al., 2006). The hydroxyl radical generating capacity of outdoor PM has been measured over the last decade (Shi et al., 2003a, Shi et al., 2003b, Kunzli et al., 2006, Boogaard et al., 2012, Yang et al., 2015). Given that people are typically exposed to indoor pollutants for much more time than outdoor pollutants, it is important to also determine the oxidative potential of particles collected from indoor environments. This study is the first to measure the hydroxyl radical generating capacity of indoor PM.

2 MATERIALS/METHODS

Total suspended particle (TSP) samples were collected simultaneously inside and outside an unoccupied 3-bedroom manufactured test house built in 2002 and located on the campus of the National Institute of Standards and Technology (NIST) in Maryland, USA. The house has a floor area of 140 m^2 and a volume of 340 m^3 (Rim et al., 2013). Particles were collected over a 4-day period on triplicate Teflon filters (37 mm) using air sampling pumps calibrated to run at 20 L/min. Indoor particles were collected 1 m above the floor in the centrally located kitchen area of the house, whereas outdoor particles were collected 1.5 m above the ground in front of the house. The house heating ventilation and air-conditioning (HVAC) system was operating on thermostatic control during all sampling periods, with the HVAC fan cycling with the thermostat in these tests. Indoor and outdoor particle counts were measured with an optical particle counter. Air change rates were measured using a tracer gas (SF_6) decay method (ASTM E741, 2011). Relative humidity and temperature were monitored inside and outside the house. Wind speed and direction were also recorded.

Particle suspensions were prepared by placing each filter in a microcentrifuge tube with 1.5 ml nanopure water and vortexing for 2 h at 2000 rpm (33.3 Hz). An aliquot of the particle suspension was mixed with hydrogen peroxide (H_2O_2) and the spin trap 5,5-dimethyl-1-pyrroline-*N*-oxide (DMPO) to make a total volume of 100 μl with 125 mmol/L H_2O_2 and 200 mmol/L DMPO. The mixture was shaken in the dark before being transferred to a 50 μl capillary and measured with a Bruker Elexsys E500 electron paramagnetic resonance (EPR) spectrometer[1]. The EPR spectra were recorded at room temperature using the following instrumental conditions: modulation frequency, 100 kHz; modulation amplitude, 1.0 G (10^{-4} T); receiver gain, 70 dB; time constant, 20 ms; conversion time, 20 ms; sweep time, 20.97 s; center field, 3340 G (0.334 T); sweep width, 80 G (8×10^{-3} T); number of points, 1024; attenuation, 15 dB; and, number of scans, 3. The oxidative potential of each PM sample (OP^{EPR}) was calculated from the sum of the area under the four peaks in the characteristic 1:2:2:1 DMPO-•OH quartet signal and expressed in arbitrary units divided by the sampled air volume.

3 RESULTS AND DISCUSSION

The oxidative potential of indoor and outdoor particles collected at the test house is given in Table 1, along with the mean measured air change rate during each sampling period. The OP^{EPR} of indoor particles was significantly different from the OP^{EPR} of outdoor particles using the Wilcoxon matched-pairs signed-ranks test (p=0.043). Nonetheless, the OP^{EPR} of indoor and outdoor particles appears to be correlated (Spearman's rho=0.90, p=0.037). The mean ratio of OP^{EPR} of indoor particles to the OP^{EPR} of outdoor particles was 72 % (± 23 % S.D.) on a sampling volume basis. The OP^{EPR} of indoor particles may be lower than that of outdoor particles on a sampling volume basis due to the removal of particles through the building envelope, to indoor surfaces, to the duct work, and by the space conditioning system filter. The HVAC filter had a minimal particle removal efficiency in the particle size ranges relevant to the indoor environment at the test house. No significant difference was observed in the OP^{EPR} of freshly collected and 1-week-old particle samples.

[1] Certain commercial equipment or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the equipment or materials identified are necessarily the best available for the purpose.

Indoor particle counts were lower than outdoor particle counts during all the sampling periods. Given that the OP^{EPR} reported here is on a sampling volume basis (to better represent exposure as it is encountered in the airways), the OP^{EPR} of indoor particles on a mass basis may be equal to or even exceed that of outdoor particles. It is unclear how many of the indoor particles infiltrated from outdoors versus being generated indoors in the present study, but it is possible that processes taking place indoors (including emissions from building materials and consumer products, resuspension from carpets, and oxidative reactions) generate particles and secondary organic aerosols (SOA) with their own free radical generating capacity. Indoor particles can have different oxidative potential than outdoor particles because a major fraction of indoor particles come from indoor homogeneous and heterogeneous chemical reactions that are distinct from outdoor chemical reactions.

The air change rate at the house ranged from 0.26 h^{-1} to 0.40 h^{-1} during the sampling periods. These rates are in the range measured during previous studies at the manufactured test house (Nabinger and Persily, 2011). Increasing the indoor relative humidity from 25 % to 40 % did not appear to substantially influence the oxidative potential of indoor particles (sampling periods 4 and 5, respectively). Further testing is underway to better understand the influence, if any, of air change rate, relative humidity, and temperature on the oxidative potential of indoor particles.

Table 1. Oxidative potential of particles collected indoors and outdoors at the manufactured test house during sampling in 2015-2016.

Sampling period	*OP^{EPR} / m^3 [A.U.]*		*Indoor / Outdoor Ratio of Oxidative Potential [%]*	*Air Change Rate [h^{-1}]*
	Indoor	*Outdoor*		
1	1.04	2.44	43 %	-
2	1.95	2.49	78 %	-
3	7.97	8.94	89 %	0.26
4	2.35	2.48	95 %	0.32
5	2.82	5.28	53 %	0.40

- Air change rate was not measured during these sampling periods.

4 CONCLUSIONS

It is important to assess the toxicological characteristics of indoor particles. OP^{EPR} of particles may be a more health relevant measure than particle mass, count or other physicochemical characteristics. EPR has been used to determine the oxidative potential of particles collected from outdoor locations in the Netherlands (Boogaard et al., 2012, Janssen et al., 2014, Yang et al., 2015), Germany (Shi et al., 2003a, Shi et al., 2003b, Shi et al., 2006), as well as several other European locations (Kunzli et al., 2006), but no such study has been conducted for indoor particles to the knowledge of the authors. The OP^{EPR} of indoor particles was found to be, on average, about three-fourth of the OP^{EPR} of outdoor particles collected at the manufactured test house at NIST. The OP^{EPR} of indoor and outdoor particles appears to be correlated, but it is unclear how much of the OP^{EPR} of the particles collected indoors was due to particles that infiltrated from outdoors versus being generated indoors. Controlled experiments are being conducted to assess the effect of indoor environmental conditions (such as relative humidity, temperature and air change rate) and indoor sources on the OP^{EPR} of indoor particles.

ACKNOWLEDGEMENT

The authors would like to acknowledge the assistance of Dan Greb in conducting the tracer gas tests and setting up the air quality measurement equipment at the test house, as well as Dustin Poppendieck for providing input during the planning of the study.

5 REFERENCES

ASTM Standard E741, 2011, "Determining Air Change in a Single Zone by Means of a Tracer Gas Dilution," ASTM International, West Conshohocken, PA, DOI: 10.1520/E0741-11.

Bell, M. L., Samet, J. M. and Dominici, F. 2004. Time-series studies of particulate matter. *Annual Review of Public Health* 25:247-280.

Boogaard, H., Janssen, N. A. H., Fischer, P. H., Kos, G. P. A., Weijers, E. P., Cassee, F. R., van der Zee, S. C., de Hartog, J. J., Brunekreef, B., Hoek, G. 2012. Contrasts in oxidative potential and other particulate matter characteristics collected near major streets and background locations. *Environmental Health Perspectives*, 120, 2, 185-191.

Borm, P. J. A., Kelly, F., Kunzli, N., Schins, R. P. F. and Donaldson, K. 2007. Oxidant generation by particulate matter: from biologically effective dose to a promising, novel metric. *Occupational and Environmental Medicine* 64:73-74.

Janssen, N. A. H., Yang, A., Strak, M., Steenhof, M., Hellack, B., Gerlofs-Nijland, M. E., Kuhlbusch, T., Kelly, F., Harrison, R., Brunekreef, B., Hoek, G., Cassee, F. 2014. Oxidative potential of particulate matter collected at sites with different source characteristics. *Science of the Total Environment*, 472: 572-581.

Künzli, N., Mudway, I. S., Götschi, T., Shi, T., Kelly, F. J., Cook, S., Burney, P., Forsberg, B., Gauderman, J. W., Hazenkamp, M. E., Heinrich, J., Jarvis, D., Norbäck, D., Payo-Losa, F., Poli, A., Sunyer, J., Borm, P. J. A. 2006. Comparison of oxidative properties, light absorbance, and total and elemental mass concentration of ambient $PM_{2.5}$ collected at 20 European sites. *Environmental Health Perspectives*, 114, 5: 684-690.

Nabinger, S. and Persily, A. 2011. Impacts of airtightening retrofits on ventilation rates and energy consumption in a manufactured home. *Energy and Buildings* 43:3059-3067.

Pope, C. A., Turner, M. C., Burnett, R. T., Jerrett, M., Gapstur, S. M., Diver, W. R., Krewski, D. and Brook, R. D. 2015. Relationships Between Fine Particulate Air Pollution, Cardiometabolic Disorders, and Cardiovascular Mortality. *Circulation Research* 116:108-U258.

Rim, D., Wallace, L. A., Persily, A. K. 2013. Indoor ultrafine particles of outdoor origin: Importance of window opening area and fan operation condition. *Environmental Science and Technology*, 47: 1922-1929.

Shi, T., Knaapen, A. M., Begerow, J., Birmili, W., Borm, P. J. A., Schins, R. P. F. 2003a. Temporal variation of hydroxyl radical generation and 8-hydroxy-2'-deoxyguanosine formation by coarse and fine particulate matter. *Occupational and Environmental Medicine*, 60: 315-321.

Shi, T., Schins, R. F. P., Knaapen, A. M., Kuhlbusch, T., Pitz, M., Heinrichd, J., Borm, P. J. A. 2003b. Hydroxyl radical generation by electron paramagnetic resonance as a new method to monitor ambient particulate matter composition. *Journal of Environmental Monitoring*, 5: 550-556.

Shi, T., Duffin, R., Borm, P. J. A., Li, H., Weishaupt, C., Schins, R. P. F. 2006. Hydroxyl-radical-dependent DNA damage by ambient particulate matter from contrasting sampling locations. *Environmental Research*, 101: 18-24.

Yang, A., Hellack, B., Leseman, D., Brunekreef, B., Kuhlbusch, T. A. J., Cassee, F. R., Hoek, G., Janssen, N. A. H. 2015. Temporal and spatial variation of the metal-related oxidative potential of $PM_{2.5}$ and its relation to the $PM_{2.5}$ mass and elemental composition. *Atmospheric Environment*, 102: 62-69.

Virtual Factory Framework for Supporting Production Planning and Control

Deogratias Kibira[1], Guodong Shao[2]

[1]Department of Industrial and System Engineering, Morgan State University, Baltimore, MD, U.S.A
deogratias.kibira@morgan.edu
[2]Engineering Laboratory, National Institute of Standards and Technology (NIST)
Gaithersburg, U.S.A
gshao@nist.gov

ABSTRACT
Developing optimal production plans for smart manufacturing systems is challenging because shop floor events change dynamically. A virtual factory incorporating engineering tools, simulation, and optimization generates and communicates performance data to guide wise decision making for different control levels. This paper describes such a platform specifically for production planning. We also discuss verification and validation of the constituent models. A case study of a machine shop is used to demonstrate data generation for production planning in a virtual factory.

Keywords: Virtual factory · Simulation · Production planning and control

1 Introduction

Conventional simulation tools are generally limited in their ability to capture and analyze multiple decision levels and system configurations (Bal et al. 2009). A virtual factory, on the other hand, creates an integrated model that reproduces scenarios of information flow and capable of generating multi-level metrics to guide users in decision- making. These decisions can among others increase agility and productivity by reducing product realization time (Colledani et al. 2013). Virtual factories have been constructed to aid manufacturing system design, implementation, and modification (Yang, et al. 2015).

Besides designing production systems and products, Choi et al. (2015) sees the potential of a virtual factory to predict, solve, and manage problems during production, which corresponds with the vision for a virtual factory as enabler of system design, training, production planning, maintenance, data analytics, and performance measurement. It is our view that the virtual factory's ability to integrate engineering tools and models such as simulations, design data, and optimizations could improve production planning activities.

Kibira, Deogratias; Shao, Guodong; Johansson, Bjoern.
"Framework for Standardization of Simulation Integrated Production Planning."
Paper presented at the Winter Simulation Conference, Arlington, VA, Dec 11-Dec 14, 2016.

As such, this paper focuses on operations and performance monitoring, particularly production planning.

The rest of the paper is organized as follows. Section 2 reviews literature related to virtual factory technology, application of virtual factories, and verification and validation (V&V) concepts for the virtual factory. Section 3 describes a role of virtual factory for production planning as per control levels defined in the ISA-95 standard. Section 4 presents a demonstration case of a virtual factory. Section 5 presents final discussion and conclusion.

2 Related Work and Virtual Factory Validation

A virtual factory is composed of multi-level, multi-resolution models that are typically developed by different methods and tools. This section overviews technologies employed for developing a virtual factory, various applications, and verification and validation issues.

Technology requirements for a virtual factory: Virtual data management, automatic model generation, static and dynamic simulation, and integration and communication are paramount to realizing a virtual factory (Choi et al. 2015; Wenbin et al. 2002). Most software tools are, in general, not supplied with these capabilities making developing a virtual factory challenging. The situation has, however, been recently improving with emergence of modeling, computation, communication, and integration technologies and standards (Jain et al. 2015). Indeed, much related literature centers on technologies for enabling the virtual factory. A few of these technologies are overviewed next.

Overview of technologies and purpose of developing virtual factories: To enhance conventional simulations for a virtual factory, Bal et al. (2009) used the PROSA architecture for modeling controls while the Quest simulation tool models the physical elements. To integrate models and enhance communication, Hints et al. (2011) developed a software tool named Design Synthesis Module. Terkaj et al. (2015) produced an ontology for a virtual factory to aid planning decisions. While Ghani (2013) developed an integrative tool to match low-level machine-component activities with targets set by aggregate planning.

Previous virtual factory models: A valid virtual factory should generate consistent data at different levels of model resolution. Shao et al. (2014) developed and validated a virtual model for generating energy usage data for machining operations. Furthering this research, Jain et al. (2015) uses a two-tailed z-test to prove statistical concurrence of experimental results from a virtual factory at both the machine and manufacturing cell levels of detail.

Verification and validation of virtual factory models: To ensure that a virtual factory is accurate for its intended purpose, V&V of constituent models and related data has to be carried out (Sargent 2007). When developing and applying formal V&V methods, key features to distinguish about models are (1) deterministic or stochastic, (2) analytical or simulated, and (3) computationally efficient or computationally expensive.

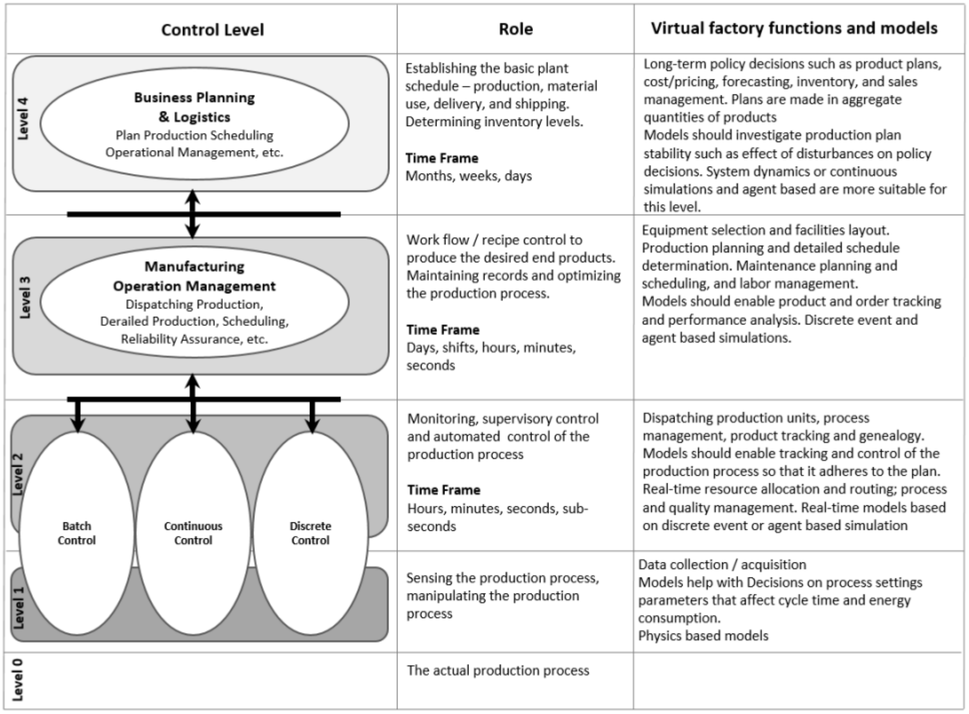
When carrying out formal V&V, Uncertainty Quantification (UQ) needs to be considered for better correctness and appropriateness (Roy 2011). Uncertainties can be epistemic or aleatoric in nature. Epistemic uncertainties arise from ignorance of involved processes, such as invalid assumptions in modeling. Aleatory uncertainties arise from inherent variability in processes, such as physical properties of a system. Model fidelity and data availability typically vary greatly across different system levels of resolution. This issue complicates both the computation of metrics that describe process performance, and decision-making based upon those metrics. V&V of a virtual factory as well as UQ can be achieved through intermediation environment, such as one created by Hibino et al. (2006) to synchronize collected data and virtual factory computed data.

3 A Virtual Factory Approach to Multi-Level Production Planning

The virtual factory concept uses the ISA-95 standard (ANSI 2013) to specify decision levels that define functions supporting multi-level production planning. This standard was developed for all types of industries, representing different manufacturing processes, such batch, continuous, discrete, and repetitive processes. As such, the description of the virtual factory herein should likewise be universally applied.

Framework and role of models: Figure 1 shows the functional hierarchical levels of ISA-95 as well as virtual factory roles at each level. At level 4, an aggregate plan is developed over a long-term planning horizon that is then investigated for stability using system dynamics (Sterman, 2000). Level 3 covers short to mid-term plans to determine actual start and finish times of individual product batches. Level 2 models make decisions on activities such as resource allocations. Level 1 is the manipulation of production process (level 0) to achieve required output. Data is collected in real-time at level 0 to update various models.

Multi-level performance analysis and improvements using the virtual factory: A production planning problem is often formulated to optimize objectives such as minimize late orders, minimize inventory, or maximize resource utilization. These objectives are basis for Key Performance Indicators (KPIs) which, along with metrics and constituent measures, are communicated and monitored. Decisions are then made to maintain them within a target performance envelop. The relationship between data, metrics and KPIs at different levels can be numerical, analytical, or heuristic influence. With heuristic influence, a KPI is expressed in terms of supporting data, parameters, metrics or other KPIs. The direction of change (increase or decrease) in the dependent KPI is investigated through the relationship equation. The Supply Chain Operations Reference (SCOR) model (SCC 2012) adopts this approach by taking KPIs and performs a metrics decomposition, performance diagnosis, or metrics root-cause analysis. SCOR then constructs a metrics dependency tree of multiple measures that would generally be generated by different models within the virtual factory.



Control Level	Role	Virtual factory functions and models
Level 4 **Business Planning & Logistics** Plan Production Scheduling Operational Management, etc.	Establishing the basic plant schedule – production, material use, delivery, and shipping. Determining inventory levels. **Time Frame** Months, weeks, days	Long-term policy decisions such as product plans, cost/pricing, forecasting, inventory, and sales management. Plans are made in aggregate quantities of products Models should investigate production plan stability such as effect of disturbances on policy decisions. System dynamics or continuous simulations and agent based are more suitable for this level.
Level 3 **Manufacturing Operation Management** Dispatching Production, Derailed Production, Scheduling, Reliability Assurance, etc.	Work flow / recipe control to produce the desired end products. Maintaining records and optimizing the production process. **Time Frame** Days, shifts, hours, minutes, seconds	Equipment selection and facilities layout. Production planning and detailed schedule determination. Maintenance planning and scheduling, and labor management. Models should enable product and order tracking and performance analysis. Discrete event and agent based simulations.
Level 2 Batch Control Continuous Control Discrete Control	Monitoring, supervisory control and automated control of the production process **Time Frame** Hours, minutes, seconds, sub-seconds	Dispatching production units, process management, product tracking and genealogy. Models should enable tracking and control of the production process so that it adheres to the plan. Real-time resource allocation and routing; process and quality management. Real-time models based on discrete event or agent based simulation
Level 1	Sensing the production process, manipulating the production process	Data collection / acquisition Models help with Decisions on process settings parameters that affect cycle time and energy consumption. Physics based models
Level 0	The actual production process	

Figure 1. Role of Virtual Factory Models According to ISA-95 Levels.

Metrics decomposition establishes a diagnostic relationship showing how metrics serve as diagnostics for dependent KPIs. For example, overall equipment effectiveness (OEE) index, as defined by ISO 22400-2 (ISO 2011), depends on availability, effectiveness, and quality rate. OEE belongs to level 3 of ISA-95 while its constituent measures can be monitored at level 2. Availability is determined by the equipment model incorporating failure and repair time study data obtained from samples of equally-spaced discrete observations during operation. The availability model can be constructed with high resolution using a programming language. Effectiveness performance model may be of low resolution constituted of run time per unit produced, number of units made, and actual production time. The quality rate is products that meet specifications compared with total units made.

Once a diagnostic relationship has been established, attention may be directed to a higher resolution of the production line model or resource responsible for a measure needing improvement while other parts of the virtual factory may remain at a lower resolution. The data, resources, and workflow through this model may then be further analyzed to balance any competing objectives that may occur. The analyst may also validate diagnosis and decision made through high visualizations of the virtual factory.

4 Case Study

This section demonstrates the monitoring of KPIs in multi-resolution models of a machining shop that exchange performance data at different decision levels using a virtual factory. At the management level, aggregate quantities of required final products to be produced are distributed to two available machine cells according to prevailing loads at each shop. Each machining shop has two major processes: turning and milling. For each process, there is more than one machine but the parts traverse both processes in the same sequence. This prototypical virtual factory is developed using AnyLogic simulation for three levels of decision control. Table 1 shows the functions and type of models employed at each level.

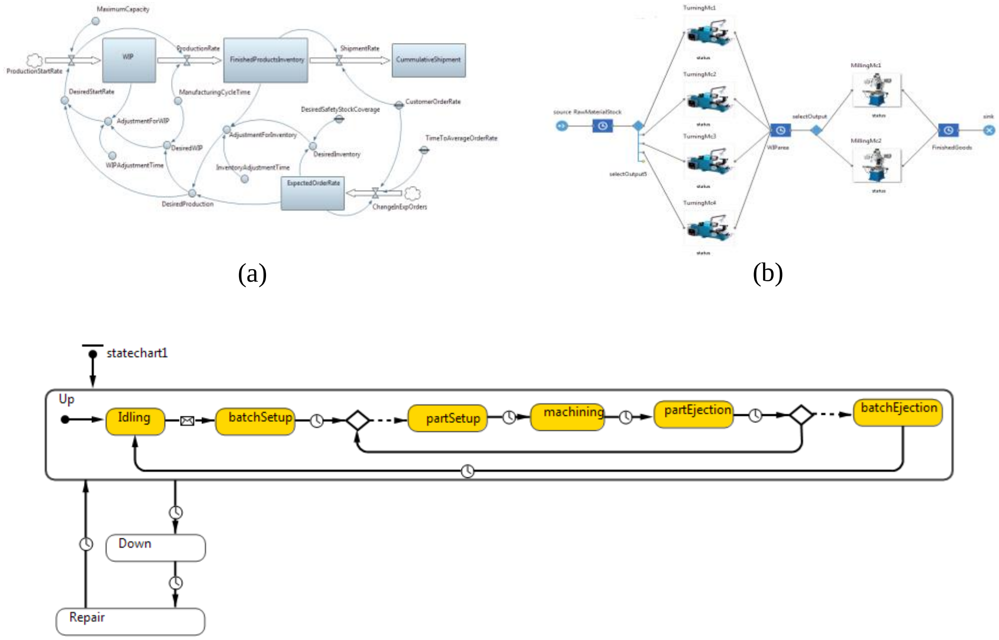
Table 1. Functions of Multi-Level Models According to ISA-95 Standard

ISA-Level	Physical system	Function	Virtual modeling method
4	Enterprise	Aggregate planning	System dynamics
3	Machine cell	Production scheduling	Discrete event simulation
2	Machine	Machine loading	Agent based modeling

Enterprise level model: This model is shown in Figure 2 (a) and is built using System Dynamics (SD). The product quantities planned for each period are input into the model to determine the production start rate at the routed shop. The production rate is a function of the production start rate and manufacturing cycle time. The production start rate is converted into inter-arrival times for the work cell model. In turn, the cycle time and work in progress levels are obtained from the machine cell model.

Machine cell model: This models the processing of a product on the shop floor. Discrete event simulation (DES) is employed, as shown in Figure 2(b). Entities enter the system from the source and routed to the first available machine for both turning and milling. The machines undergo periodic failure and repair cycles.

Machine level model: This is a model of states of a machine during normal operation. They are represented by Agent-based Modeling using statecharts in AnyLogic. Machine failure and repair cycle are indicated in the statechart shown in Figure 2 (c). When a machine is "Up", default sub-state is idling to which a machine reverts after repair or after ejection of the previous batch. Other machine states are “Down” or “Under repair” and, in these states, incoming parts cannot be routed to them. The machines undergo this cycle independently.



(a)

(b)

(c)

Figure 2. Multi-resolution models of the virtual factory

Model interactions: When these models are integrated, the SD model receives input data from DES for update to aggregate planning. In turn, DES is updated with agent based simulations of machine processes. Figure 3 shows the exchanged data. Figure 4 shows that there is enough visual concurrency in monitored generated data: work in progress levels and production quantity between models at different resolution levels.

Such data can be used, for example, to monitor and maintain planned throughput rate. According to ISO 22400-2 (ISO 2011), throughput rate = quantity produced/order execution time. Maximizing throughput in a job-shop production environment requires deploying the “shortest remaining processing time” priority rule (Panwalkar et al. 1977). If throughput rate is reduced, the causes are investigated using the constituent measures monitored at level 2 of ISA-95. These are analyzed with the discrete event simulation model. The cause could be an increase in order execution time which in turn depends on manufacturing cycle time. The causes of increase in cycle time can further be analyzed using work cell model.

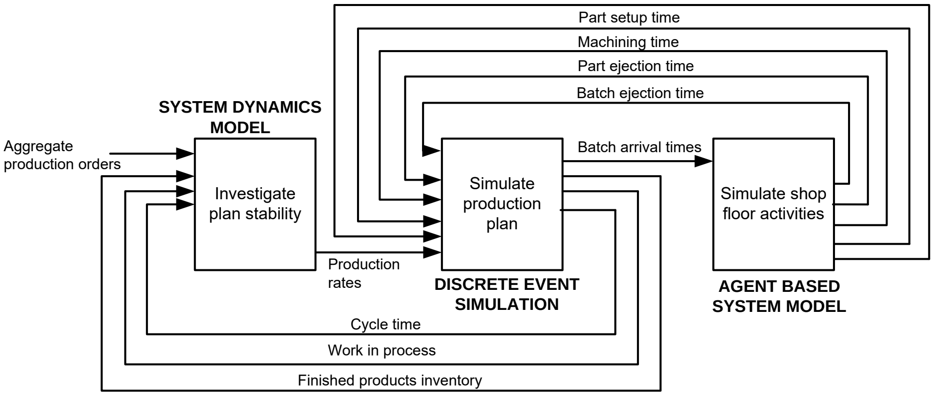


Figure 3. Data generated and exchanhged between models

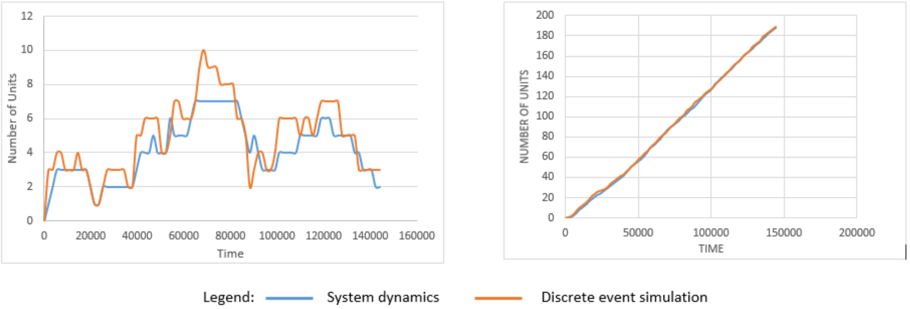


Figure 4. Work in progress and cumulative production with time for system dynamics and discrete event simulations.

5 Discussion and Conclusion

A virtual environment can be developed for generating and communicating production planning decisions from floor and optimize production, inventory, and cost objectives. Communicating performance of production plans and schedules in a virtual environment is beneficial to achievement of the smart manufacturing objectives. The industrial internet is one technology for connecting, collecting and communicating data. This framework is a first step in describing how the virtual factory can be used for developing and integrating models at different hierarchical levels. The example in this paper used a multi-method simulation software. To take advantage of strengths of different tools, a virtual factory would be developed using heterogeneous tools. Description of needed interfaces and review of existing standards will be the subject of future research work.

Acknowledgement: This effort has been sponsored in part under the cooperative agreement No. 70NANB13H153 between NIST and Morgan State University. The work described was funded by the United States Government and is not subject to copyright. The contribution of David Lechevalier of NIST in lower-level simulation work is acknowledged.

Disclaimer: No approval or endorsement of any commercial product by the National Institute of Standards and Technology is intended or implied. Certain commercial software systems are identified in this paper to facilitate understanding. Such identification does not imply that these software systems are necessarily the best available for the purpose.

6 References

1. Bal, M., & Hashemipour, M. (2009). Virtual Factory Approach for Implementation of Holonic Control Industrial Applications: A Case Study in Die-Casting Industry, *Robotics and Computer-Integrated Mfg.*, 25, 570 – 581.
2. Choi, S. Kim, B.H., & Noh, S.D. (2015). A diagnosis and Evaluation Method for Strategic Planning and Systematic Design of a Virtual Factory in Smart Mfg. Systems, *Int. J. of Precision Eng. and Mfg.*, 16, 1107-1115.
3. Colledani, M. Pedrielli, G., Terkaj, W. & Urgo, M. (2013). Integrated Virtual Platform for Mfg. Systems Design, *46th CIRP Conf. for Mfg. Systems Design*, Procedia CIRP 7, 425-430. SciVerse ScienceDirect
4. Ghani, U. Monfared, R., & Harrison, R. (2014). Integration Approach to Virtual-driven Discrete Event Simulation for Manufacturing Systems, *Int. J. of Computer Integrated Mfg.*, 8, 844-860.
5. Guan, Z., Wang, C., Wu, Y., & Shao, X. (2012). A Framework of Digital Factory System Using Multi-resolution Simulation, *Applied Mechanics and Materials,* 159, 12-17.
6. Hibino, H., Inukai, T., & Fukuda, Y. (2006). Efficient Manufacturing System Implementation based on Combination between Real and Virtual Factory. *Int. J. of Production Research*, 44, 3897-3915.
7. Hints, R., Vanca, M., Terkaj, W., Marra, E.D., Temperini, S., & Banabic, D. (2011). A virtual Factory Tool to Enhance the Integrated Design of Production Systems, *Proc. of the DET2011 7th Int. Conf. on Digital Enterprise Technology*, Athens, Greece, 28-30.

8. ISO 22400-2: (2011). *Automation systems and integration – Key performance indicators (KPIs) for manufacturing operations management – Part 2: Definitions and descriptions of KPIs*.
9. Jain, S., Lechevalier, D., Woo, J., & Shin, S-J. (2015). Towards a Virtual Factory Prototype, *Proc. of the 2015 Winter Simulation Conf.*, L. Yilmaz, W. K. V. Chan, I. Moon, T. M. K. Roeder, C. Macal, and M. D. Rossetti, eds., 2207-2218.
10. Jain, S., Shao, G. (2014). Virtual Factory Revisited for Manufacturing Analytics, *Proc. of the 2014 Winter Simulation Conf.*, Tolk, A., Diallo, S. Y., Ryzhov, I. O., Yilmaz, L., Buckley, S. and Miller, J. A. (eds.), 887-898.
11. Jain, S. Siguroardottir, S., Lindskog, E., Andersson, J., Skoog, A., & Johansson, B. (2013). Multi-resolution Modeling for Supply Chain Sustainability Analysis, *Proc. of the 2013 Winter Simulation Conf.*, Pasupathy, R., Kim, S.-H., Tolk, A., Hill, R., and Kuhl, M. E., eds., 1996-2007.
12. Lee, C.G. & Park, S.C. (2014). Survey on the Virtual Commissioning of Manufacturing Systems, *J. of Computational Design and Eng.*, 1, 213-222.
13. Mourtzis, D., Papakostas, N., Mavrikios, D., Makris, S., & Alexopoulos, K. (2013). The Role of Simulation in Digital Manufacturing: Applications and Outlook, *Int. J. of Computer Integrated Mfg.*, 28, 3-24.
14. Panwalkar, S. S. & Iskander, W. (1977). A Survey of Scheduling Rules, *Operations Research*, 25(1), 45-61.
15. Roy, C. J. & Oberkampf, W. L. (2011). A Comprehensive Framework for Verification, Validation, and Uncertainty Quantification in Scientific Computing. *Computer Methods in Applied Mechanics and Eng.*, 200(25–28), 2131-2144.
16. Sargent, R. (2007). Verification and Validation of Simulation Models, *Proc. of the 2007 Winter Simulation Conf.*, Henderson, S. G, Biller, B., Hsieh, M.-H., Shortle, J. Tew, J. D., and Barton, R. R. (eds). 124-137.
17. Shao, G., Jain, S., Shin, S.-J. (2014). Data Analytics using Simulation for Smart Manufacturing. *Proc. of the 2015 Winter Simulation Conf.*, A. Tolk, A., S. D. Diallo, I. O. Ryzhov, L. Yilmaz, S. Buckley, & J. A. Miller, eds., 2192-2203.
18. Sterman, J.D. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World*, Irwin, McGraw-Hill.
19. Terkaj, W., Tolio, T., & Urgo, M. (2015). A Virtual Factory Approach for in Situ Simulation to Support Production and Maintenance Planning, *CIRP Annals - Mfg. Technology*, 64, 451–454.
20. Tolk, A. (2013). Interoperability, Composability, and Their Implications for Distributed Simulation: Towards Mathematical Foundations of Simulation Interoperability, *IEEE/ACM 17th Int. Symposium on Distributed Simulation and Real Time Applications (DS-RT*), 3-9.
21. Venkateswaran, J. & Y. Son. (2004). Distributed and Hybrid Simulations for Manufacturing Systems and Integrated Enterprise. In *Proc. of the 2004 Industrial Eng. Research Conference.*

22. Wenbin, Z., Xiumin, F., Juanqi, Y., & Pengsheng, Z. (2002). An Integrated Simulation Method to Support Virtual Factory Engineering. *Int. J. of CAD/CAM*, 2, 39-44.
23. Yang, X., Malak, R. C., Lauer, C., Weidig, C., Hagen, H., Hamann, B., Aurich, J. C., & Kreylos, O. (2015). Manufacturing System Design with Virtual Factory Tools, *Int. J. of Computer Integrated Manufacturing*, 28, 25-40.

Proceedings of the 2015 Winter Simulation Conference
L. Yilmaz, W. K. V. Chan, I. Moon, T. M. K. Roeder, C. Macal, and M. D. Rossetti, eds.

INTEGRATING DATA ANALYTICS AND SIMULATION METHODS TO SUPPORT MANUFACTURING DECISION MAKING

Deogratias Kibira

Department of Industrial and Systems Engineering
Morgan State University
1700 E Cold Spring Ln
Baltimore, MD 21251, USA

Qais Hatim
Soundar Kumara

Department of Industrial and Manufacturing Engineering
Pennsylvania State University
University Park
State College, PA 16801, USA

Guodong Shao

Systems Integration Division, Engineering Laboratory
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899, USA

ABSTRACT

Modern manufacturing systems are installed with smart devices such as sensors that monitor system performance and collect data to manage uncertainties in their operations. However, multiple parameters and variables affect system performance, making it impossible for a human to make informed decisions without systematic methodologies and tools. Further, the large volume and variety of streaming data collected is beyond simulation analysis alone. Simulation models are run with well-prepared data. Novel approaches, combining different methods, are needed to use this data for making guided decisions. This paper proposes a methodology whereby parameters that most affect system performance are extracted from the data using data analytics methods. These parameters are used to develop scenarios for simulation inputs; system optimizations are performed on simulation data outputs. A case study of a machine shop demonstrates the proposed methodology. This paper also reviews candidate standards for data collection, simulation, and systems interfaces.

1 INTRODUCTION

The manufacturing environment is characterized by continuously changing conditions that affect processes, operations, and priorities. Therefore, evaluating a manufacturing system performance to decide course of action is a challenging task. To monitor performance, today's smart manufacturing systems are installed with ubiquitous sensors and other smart systems that are collecting large volumes and varieties of data. The collected data has also issues of veracity, certainty, and validity for intended purpose. Furthermore, the data are interrelated and influenced by many factors. Traditional data analysis methods alone, including simulation, fail to transform this high-volume, continuously streaming data into knowledge for decision support. Data analytics methods are being advanced and applied to understanding how to utilize the high-volume, high-variety data that is being collected from today's manufacturing

Kibira, Deogratias; Hatim, Qataris; Shao, Guodong; Kumara, Soundar.
"Integrating Data Analytics and Simulation Methods to Support Manufacturing Decision Making."
Paper presented at the Winter Simulation Conference, Huntington Beach, CA, Dec 6-Dec 9, 2015.

systems. Data analytics methods, especially data mining, have been targeting important areas in manufacturing such as product quality (Skormin et al. 2002), production planning and scheduling (Chen 2001), and manufacturing process optimization (Gröger et al. 2012; Zheng et al. 2014). Data mining is the process of identifying knowledge hidden in large amounts of data and can be useful to support decision making. Considering the wide range of possible system behaviors that depend on inputs, data mining tools can uncover important parameters that are associated with a given type of behavior. The discovered associations between inputs and behavior can further be analyzed using simulation models to determine the parameter settings that result in the best system performance. As a consequence, better decisions can result when data mining is integrated with simulation models.

Traditionally, decision makers use simulation models to represent a real-world system in a virtual environment, and to test and evaluate the system's performance under different operating conditions. Applying a simulation analysis approach involves collecting data and developing a model using an appropriate simulation software tool (Banks et al. 2009). Evaluations are done based on performance indicators such as capital investments, asset utilization, and environmental impacts (Dudas et al. 2009). The selected indicators largely depend on the performance objectives of the organization and may be different for each simulation study. Because simulation users often need to select system inputs from the large number of possible alternatives, simulation are often combined with optimization methods.

Optimizations apply mathematical techniques for modeling real-world problems and solve problems based on specific objectives to produce actionable recommendations. Brady and Yellig (2005) proposed two approaches for integrating simulation with optimization. The first one is to construct an external optimization framework around the simulation model. The second one is an internal approach to investigate the relationships and interactions among system variables within the simulation model. The tracking features within the tools can be used for the purpose. We use the first approach in this paper.

In summary, we note two issues for using the large volume of collected data to improve the performance of a manufacturing system with simulation. The first one is to determine important parameters affecting the required performance from the data. The second is to determine the best input settings of the parameters to optimize the process. The collected data contains intricate dependencies, which requires automated tools to extract useable information. In this paper we propose a methodology utilizing the strengths of data mining, simulation, and optimization for decision guidance in manufacturing systems. Data mining methods first extract those parameters and variables that affect system performance. We then use the identified parameters and associated data as simulation inputs to predict system performance for defined scenarios. Subsequently, optimization methods are used to determine the best parameter settings, from alternatives generated by the simulation that lead to actionable recommendations. We believe that the synergistic effect of data mining, simulation, and optimization can support manufacturing decision making in the face of big data and system complexity.

The rest of the paper is organized as follows: Section two reviews related work, Section three describes the proposed methodology. Section four shows how the methodology can be used for a machining job shop. Section five concludes the paper and discusses the future work.

2 RELATED WORK AND STANDARDS

This section reviews the existing work and information standards related to the proposed methodology of this paper. Simulation provides an accurate projection of manufacturing system behavior. However, determining the set of inputs that optimize system performance is challenging because simulation optimization necessitates that the decision maker fully understands both the optimization approach and the underlying stochastic processes (Andradóttir 1998). Researchers such as Skoogh et al. (2010) published the GDM-Tool for processing input-streaming data with the purpose of enabling the reuse of simulation models. This tool does not process input data for optimizing defined system performance. Secondly, the large volume of data, the number of possible input parameters, and the variety of their interactions make it difficult to choose the best combination of data inputs relevant for the desired

Kibira, Deogratias; Hatim, Qataris; Shao, Guodong; Kumara, Soundar.
"Integrating Data Analytics and Simulation Methods to Support Manufacturing Decision Making."
Paper presented at the Winter Simulation Conference, Huntington Beach, CA, Dec 6-Dec 9, 2015.

objectives. Data mining uses techniques such as classification, clustering, association, and sequential pattern discovery to discover knowledge hidden in large volumes of data. Recently, researchers have recognized the potential benefit of integrating data mining, simulation, and optimization (Better et al. 2007). Data mining methods, applied to manufacturing data, discover knowledge and patterns in the data and relationships between the data that can be represented in simulation models (Alnoukari et al. 2010).

Previous work in integrating data mining and simulation include software project management (Garcia et al. 2008). In this application, the authors use an association rule mining algorithm to build a model that relates management policy attributes to quality, time, and effort in software development. The applications of data mining in simulation modeling are classified into two modeling types (1) micro-level modeling, which uses data mining techniques on historical data to tune input parameters and (2) macro-level modeling that uses the data mining techniques to analyze data to reveal patterns that could help better model the overall behavior of the system (Remondino et al. 2005). In this paper, we use the latter approach and use the discovered patterns as inputs to simulation and optimization models to obtain input parameter values that provide optimal system performance.

Optimizations are done by formulating problems using operations research methods including metaheuristics and mathematical programming (Olafsson et al. 2008). Carson and Maria (1997) categorized optimization methods into gradient-based search methods, stochastic optimization, response surface methodology, heuristic methods, and statistical methods. For manufacturing, simulation-based optimization methods include response surface, direct search, perturbation analysis, and evolutionary algorithms (Azadivar 1992; Paris et al. 2001). Tools have been developed for analysis of simulation output data (Bogon et al. 2012). This process is classified external optimization, in that it is done outside the simulation model. Simulation tools also incorporate algorithms to provide optimization capability.

Implementing the methodology with multiple methods and tools requires standards. Data and system interface standards are the foundation for information representation, model composition, and system integration. Standards are used to measure, collect, represent, and exchange the data relevant to data analytics, simulation, and production. Currently, different data formats are used in industry. Sample standards for manufacturing systems at different levels follow (Jain and Shao 2014):

- ISA-95 is developed for the integration of enterprise and control systems under coordination efforts by the International Society for Automation (ISA) (ANSI 2010).
- The OAGIS standard, from the Open Applications Group, establishes integration scenarios for a set of applications including enterprise requirements planning (ERP), manufacturing execution system (MES), and Capacity analysis (OAGIS 2014). While OAGIS does not cover full enterprise objects, it is focused on the required models for data exchange.
- Business to Manufacturing Markup Language (B2MML) is a set of eXtensible Markup Language (XML) schemas that implement the data models in the ISA-95 standard. B2MML enables businesses to integrate their Manufacturing Execution System (MES) solutions with their Enterprise Resource Planning (ERP) systems.
- Core Manufacturing Simulation Data (CMSD) is a standard to help achieve simulation applications interoperability (SISO 2012). CMSD enables exchanging shop floor simulation data with manufacturing applications such as ERP, Master Production Schedule, and MES.
- MTConnect is a middleware standard that enables the real time, automated data extraction from numerically-controlled machine tools using the XML standard (AMT 2013).
- Emerging Data analytics standard: PMML is a data mining standard developed by the Data Mining Group (DMG), an independent, vendor-led consortium. PMML describes the exchange of statistical and data mining models. With PMML, it is easy to develop a model on one system using one application and deploy the model on another system using another application (DMG 2014).

3 PROPOSED METHODOLOGY

This section describes the methodology illustrated in Figure 1. The first step is formulating the problem and specifying high-level performance objectives, indicators, and metrics. This is followed by acquiring domain knowledge of the manufacturing system, processes, performance indicators, and metrics. Next, a conceptual model needs to be developed for understanding the requirements for modeling, simulation, and analysis. Then, data analytics methods need to be applied to the data collected to extract parameters and developing scenarios for inputs to the simulation model. Actionable recommendations are obtained through simulation optimizations. Each step of the methodology is described next.

Two features distinguish this methodology from traditional approaches (1) input of a large volume and variety of constantly streaming data collected from the system using smart devices, and (2) using association and classification methods of data mining to determine important parameters associated with given performance indicators. The indicators can differ with every industry or occasion. As indicated in the introductory section, traditional simulation approaches would fail to be applied to this type data.

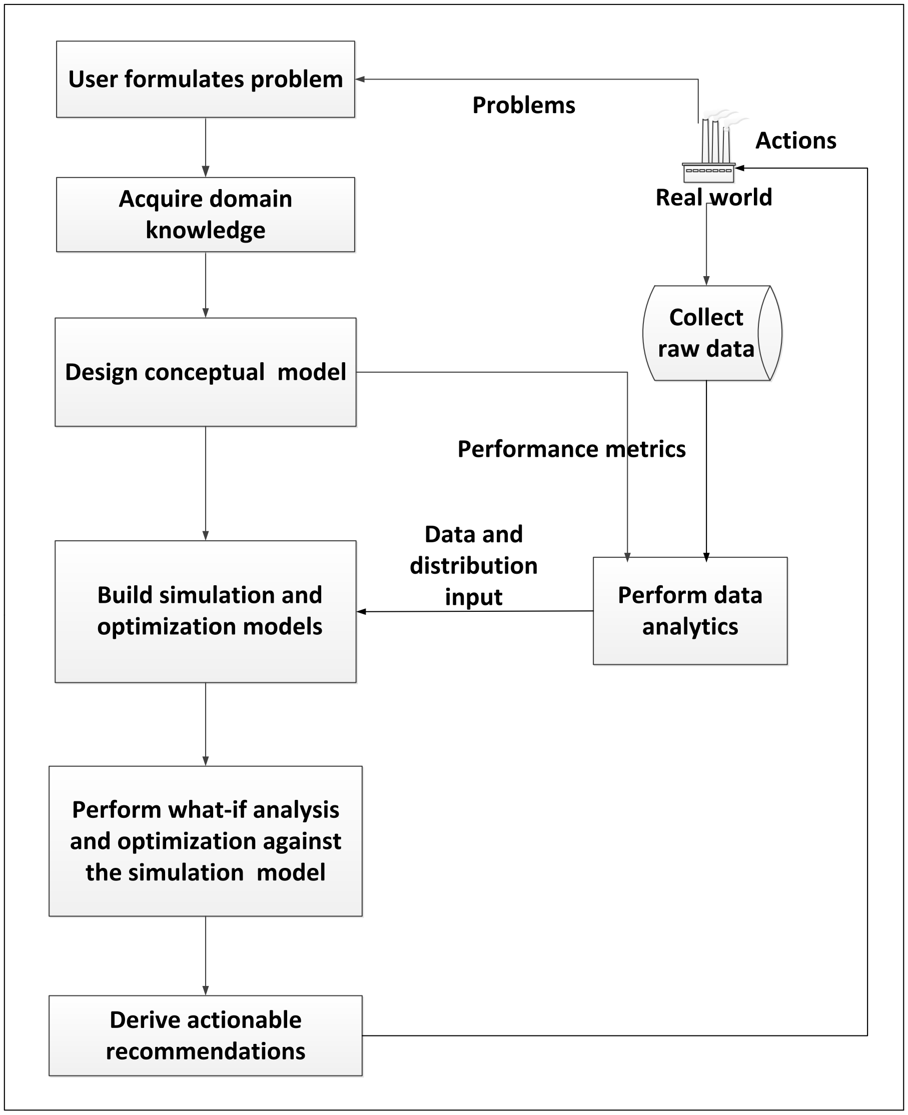

User formulates problem
Problems
Actions
Real world
Acquire domain knowledge
Collect raw data
Design conceptual model
Performance metrics
Data and distribution input
Build simulation and optimization models
Perform data analytics
Perform what-if analysis and optimization against the simulation model
Derive actionable recommendations

Figure 1: Procedure for data analytics and simulation optimizations.

Kibira, Deogratias; Hatim, Qataris; Shao, Guodong; Kumara, Soundar.
"Integrating Data Analytics and Simulation Methods to Support Manufacturing Decision Making."
Paper presented at the Winter Simulation Conference, Huntington Beach, CA, Dec 6-Dec 9, 2015.

3.1 Formulate the Problem

Formulate the problem by receiving problem input data from the real world, identify the system or processes of interest and specify performance goals by defining indicators and metrics at a high level. Identify relevant resources, products, and activities. System conditions, constraints, and decision variables should also be defined.

3.2 Acquire Domain Knowledge

Acquire or obtain from domain experts, knowledge related to the problem including performance indicators, metrics, conditions, and targeted goals. If the goal is agility performance, for example, the user would research on the relationship between agility and collectable data. The user would also study factors that define and determine agility performance.

3.3 Design a Conceptual Model

Develop a conceptual model, which is a simplified representation of the identified problem. It provides the right level of abstraction that satisfies the modeling objectives and focuses on the metrics of concerns. It helps modelers better understand the problem and prepare for modeling and analysis. When designing a conceptual model, the following typical questions need to be answered to help users abstract the problem and plan the detailed modeling (1) What are the components (systems/processes) that need to be modeled?, (2) What are the inputs and outputs of each component?, (3) What are the relationships between components?, (4) What are the metrics and indicators?, and (5) What are the data requirements for the metrics? The conceptual models help identify requirements for data collection.

3.4 Collect Data

Collect raw data using various devices and methods such as sensors, bar codes, vision systems, meters, and radio frequency identification (RFID). Gröger et al. (2012) classified data into manufacturing process data and operational data. Process data is made up of execution data; i.e., machine and production events recorded by the MES. Process data from machine tools include processing time, idle time, loading time, energy consumption, machine setting, tool, and tear down time. MTConnect is one standard that can be used for this purpose. Operational data mainly encompasses Computer-aided design (CAD), Computer-aided Process Planning (CAPP), and ERP data. For data storage, Structured Query Language (ISO/IEC 2011) is one means of storing and retrieving data. The data is represented in neutral format such as XML.

3.5 Use Data Analytics Methods

Select appropriate data analytics methods that should (1) use the collected data to identify parameters that are related to defined performance, (2) be adaptable to different data and performance objectives, and (3) perform the data analysis.

Data mining methods are used because the complexity of the shop floor data makes it difficult to establish analytical relationships between the input variables and performance measures. Choosing the appropriate data mining method depends on the particular problem. For example, association methods should be used to determine whether there is a relationship between two data sets. Classification methods should be used to identify specific characteristics or attributes of a data set and to determine whether a new data item belongs to a group that exhibits these attributes (Better et al. 2007). Our approach is to first define performance indicators and use the association method to determine, from the collected data, the particular parameters that impact the performance indicator. Each performance objective or sets of objectives form distinct groups. These objectives are defined before the data mining process and the corresponding groups are known a priori. The determination of the relevant data type acts as a data preparation for input to the simulation model.

If y is the performance indicator, we can represent y as a function $y = f(x, w)$,

where $x = (x_1, x_2, x_3, \ldots x_d)^T$ denotes the set of parameters that impact energy use and w denotes the weight of the parameters.

3.6 Perform Simulation Modeling and Optimization

Construct the simulation and optimization models, incorporating sufficient detail to evaluate performance. There are a number of commercial simulation tools available on the market. In performing optimization, we need to define the decision variables, x and optimization criteria. Also, define constraints and restrictions on values of decision variables.

In example of optimizing energy consumption:

If $F(x)$ = function that expresses the total energy consumption
$A(x)$ = matrix of production needs for products
b = minimum requirements for each product
L_{min} = lower limit
L_{max} = upper limit

The formulation would be as follows:

Minimize $F(x)$
Subject to $A(x) \geq b$ (constraints)

$$L_{min} \leq x \leq L_{max}$$

The optimization model can also use any optimization tools supplied with simulation software. Simulation quantifies the impact of the inputs used to run the system. By making several runs of different inputs and what-if scenarios, the tools systematically compare the results of each current run with those of past runs to decide on a new set of input values until the optimum is gradually approached. The CMSD standard can be used to model the input data for the simulation modeling.

3.7 Derive Actionable Recommendations

Interpret and translate the output from the optimizations into actionable recommendations that can be executed on the manufacturing system. The users also need to check if the recommended actions conflict with already perceived knowledge about the system and resolve this conflict.

4 CASE ANALYSIS FOR IMPLEMENTING THE METHODOLOGY

This section describes how the methodology was demonstrated using a machining job shop. It is a simplified setting to showcase the steps of the methodology and does not include master data from the ERP system. This section (1) describes the production process, (2) defines performance objectives and, (3) describes how the proposed methodology was applied to achieve the performance objectives.

The job shop produces a variety of custom-designed metal products. The shop floor consists of a number of machine tools including a turning lathe, a mill, a drill press, and a boring machine. When an order is received, the users can decide to focus on any or all of these performance objectives (1) minimize costs (e.g., labor, cutting tool, and energy costs), (2) minimize resource usage (e.g., material, energy, and water), and (3) maximize productivity. Each part has a process plan. However, the sequencing of orders or of parts at a machine or a station can vary depending on the users' objectives. Some machines can perform more than one process. The choice of a machine for a process will produce different impacts on resource (materials and energy) consumption and processing time.

The machines can have different setup parameter settings such as feed rate, cutting speed, and depth of cut. These also affect cycle time, production rate, cost, and resource consumption. Figure 2 shows the production flow through the shop. Data are collected on resources, products, environment, and decision rules. Because of multiple objectives and large volume of data collected, it is impossible to determine the optimal combination of sequence, machines and settings, or batch size without a tool or a systematic methodology to identify and optimize these parameters according to the required performance objective.

Formulate the problem: The problem is formulated as follows.
Objectives: optimize materials and energy consumption and productivity
Decision: obtain optimal process plan (including machines and machine settings) for manufacturing parts
Conditions/situation: consider that multiple machines can be chosen to perform an operation, multiple settings for a machine; and variable impacts can occur depending on the selected machines and settings.

Acquire domain knowledge: The following knowledge was needed before modeling: machining processes, energy consumption in machining, production scheduling in job shops, sequencing, costing of manufacturing processes, performance indicators and metrics, and performance data.

Design conceptual model: Based on the knowledge of the defined problem, a high-level conceptual model is developed to highlight the relationship between inputs and outputs. The information needs are: product design, process routes, product material, mapping product design and material to a process, machines and tools, machine setting, and a performance indicator that drives the selections above.

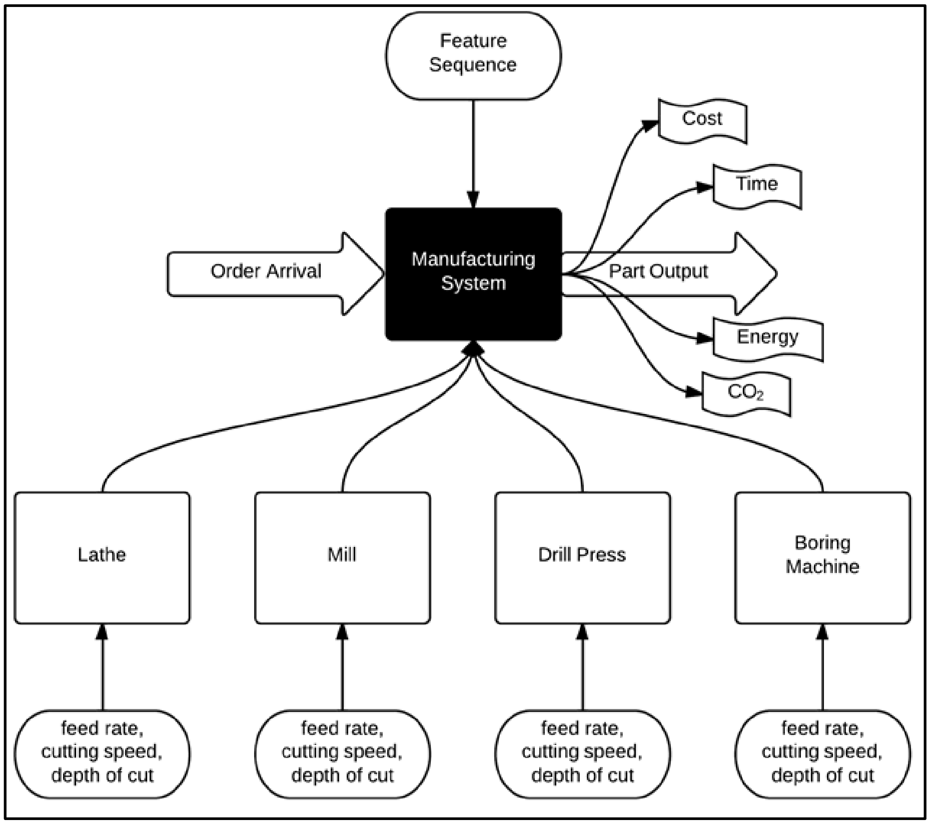

Feature Sequence
Cost
Time
Order Arrival
Manufacturing System
Part Output
Energy
CO₂
Lathe
Mill
Drill Press
Boring Machine
feed rate, cutting speed, depth of cut
feed rate, cutting speed, depth of cut
feed rate, cutting speed, depth of cut
feed rate, cutting speed, depth of cut

Figure 2: Production flow through a machining shop.

Kibira, Deogratias; Hatim, Qataris; Shao, Guodong; Kumara, Soundar.
"Integrating Data Analytics and Simulation Methods to Support Manufacturing Decision Making."
Paper presented at the Winter Simulation Conference, Huntington Beach, CA, Dec 6-Dec 9, 2015.

Collect data: Data is collected from the machines as production orders flow through the shop. The attributes of the production order are:

- product type (sub-attributes: design features, material),
- manufacturing equipment (sub-attributes: machine type for an operation, machine settings, tool, machine energy use, machine process time),
- production planning (sub-attributes: batch size, sequencing rule, part routing), and
- performance data (sub-attributes: energy consumption, production cost, production time).

Use data analytics' methods: We use association rules' techniques from data mining to discover the parameters (attributes) that have significant impact on the defined performance. For this demonstration we discover that for a given material, the parameters that affect energy consumption are (1) the machine, (2) diameter of cutter, (3) number of teeth on cutter, (4) depth of cut and, (5) feed rate.

Perform simulation modeling and optimization: We construct a discrete event simulation model of the machine shop using a simulation software tool to predict performance. For energy consumption we evaluate how a given machine and cutting tool affect the energy use without caring about other indicators. The main simulation modules are part arrival, data requirements for the part and process, the part routing to various machines, part exit, and statistics generation. Instead of a separate optimization tool, actionable recommendations are obtained by using optimization capability provided by using OptQuest that is optimization package integrated with Arena. OptQuest uses heuristics known as Tabu search, integer programming, neural networks, and scatter search for seeking within the control (input) space and converges to an optimal solution. The user controls the possible ranges of input variables and defines the objective and sets-up inputs for OptQuest. The CMSD standard can be used to model the input data for the simulation modeling. Table 1 shows the scenarios used in this simplified case. The table also displays the resulting impacts from various system inputs.

Derive actionable recommendations: We execute the simulation model for processing a part product that requires the processes: facing, grooving, threading, spot drilling, and final drilling. Each process is associated with a resource set (R); i.e., machine (designated M) and a tool (T). Three cases have been considered: predefined process plan for the features' production sequence, relaxation on the operational order for some features, and unspecified process plan. In the predefined case, each process has a pre-determined machine and cutting tool, determined to optimize a given performance objective. In case of minimum-energy-utilization objective, the machines selected are those that perform the process with minimum energy consumption. In the unspecified case, a machine is selected according to a priority rule such as machine with minimum number of parts waiting.

For each of the three cases, different process plans are tested and for each combination (production and process planning) impacts on two key performance indicators (KPIs): energy consumption and production time. Table 1 shows the energy consumption and production time data for different scenarios of process plans. The resource column shows options of machine and tools for a process; while the indicator columns show the resulting impacts. The table shows the tool-tip energy while the production time displays only the total processing time on the machines. Table 1 shows that the choice of sequence plan, operation, and resource influences the performance indicator. By resource we refer to the machine tool and cutting tool used. The results are summarized in Table 2 where the optimum inputs and settings can be selected visually. The minimum energy consumption is obtained by selecting resources $R_2R_3R_4R_6R_9$.

Table 1: Impacts of selected resources on performance indicators.

Feature Sequence Plan	Operation	Resource R_i	Sustainability Indicator	Productivity Indicator
			Machining Energy (kWh)	Production time (h)
Predefined Feature Sequence Plan	Facing	R_1= M1-T1	19.901	0.215
		R_2= M2-T5	16.205	0.014
	Grooving	R_3= M2-T4	16.205	0.014
	Threading	R_4= M1-T2	5.970	0.064
	Spot Drill	R_6= M1-T3	5.307	0.057
		R_7= M3-T7	6.336	0.292
	Drill	R_6= M1-T3	13.267	0.143
		R_9= M4-T9	8.817	0.183
Partially Defined Feature Sequence Plan	Facing	R_2= M2-T5	16.205	0.014
	Grooving	R_3= M2-T4	16.205	0.014
	Threading	R_4= M1-T2	7.793	0.060
	Spot Drill	R_6= M1-T3	6.927	0.053
	Drill	R_6= M1-T3	17.318	0.132
Undefined Feature Sequence Plan	Facing	R_2= M2-T5	16.205	0.014
	Grooving	R_3= M2-T4	16.205	0.014
	Threading	R_4= M1-T2	7.793	0.060
	Spot Drill	R_6= M1-T3	6.927	0.053
	Drill	R_6= M1-T3	17.318	0.132

Table 2: Summary of process plans for different feature sequences when minimizing energy consumption.

Feature Sequence Plan	Process Plan PP_j	Facing	Grooving	Threading	Spot Drill	Drill
Predefined Feature Sequence Plan	PP_1	R_1	R_3	R_4	R_6	R_6
	PP_2	R_1	R_3	R_4	R_7	R_6
	PP_3	R_1	R_3	R_4	R_6	R_9
	PP_4	R_1	R_3	R_4	R_7	R_9
	PP_5	R_2	R_3	R_4	R_6	R_6
	PP_6	R_2	R_3	R_4	R_7	R_6
	PP_7	R_2	R_3	R_4	R_6	R_9
	PP_8	R_2	R_3	R_4	R_7	R_9
Partially-Defined Feature Sequence Plan	PP_1	R_2	R_3	R_4	R_6	R_6
Undefined Feature Sequence Plan	PP_1	R_2	R_3	R_4	R_6	R_6

5 DISCUSSION AND FUTURE WORK

This paper has introduced a methodology that integrates data analytics, simulation, and, optimization to analyze large volumes of data for the purpose of improving decision making. Data mining extracts information - such as patterns and statistical distributions – that provides inputs to a simulation model. We use this model to develop different manufacturing scenarios and to compute various performance metrics. We then use optimization techniques to search for best input selections for those metrics. We demonstrated how to use the methodology using a case study for identifying a process plan that optimizes production cost.

Implementing this methodology requires standards that are relevant for the following purposes (1) data collection, (2) data representation, (3) model composition, and (4) system integration. Candidate standards include MTConnect, PMML, CMSD, and ISA-95. OAGIS (OAGIS 2014) can integrate applications including ERP, MES, and capacity analysis but it is more emphasized at the enterprise level. ISA-95 is more emphasized at the operations level. Further, OAGIS and ISA-95 standards were not intended to provide interfaces with simulation systems nor with each other. Future work is needed for these two standards to support simulation integrations both at shop floor level and between different planning levels in a manufacturing company. On the other hand, CMSD is developed especially for integrating simulation systems applications with other manufacturing applications. It is a candidate standard for interoperability with simulation models. More standardization efforts are needed especially for data collection, where data collected is still limited to machine tool data, representation and data mining.

For further development of this methodology, future work includes the definition and description of a framework for data collection and interface for input to data mining and simulation tools; investigation of data mining standards for the methodology; the requirements analysis for extension of existing standards for interfacing between data mining tools, simulations, optimization, and manufacturing system monitoring tools; and conducting industrial case studies to further validate the proposed methodology.

DISCLAIMER

No approval or endorsement of any commercial product by the National Institute of Standards and Technology is intended or implied. Certain commercial software systems are identified in this paper to facilitate understanding. Such identification does not imply that these software systems are necessarily the best available for the purpose.

ACKNOWLEDGMENT

This effort has been sponsored in part under the cooperative agreement No.70NANB12H284 between NIST and Pennsylvania State University and under cooperative agreement No. 70NANB13H153 between NIST and Morgan State University. The work described was funded by the United States Government and is not subject to copyright.

REFERENCES

Alnoukari, M., A. El Sheikh, and Z. Alzoabi. 2010. “An Integrated Data Mining and Simulation Solution.” *Handbook of Research on Discrete-event Simulation Environments Technologies and Application* 16: 359–380.

AMT 2013. “Getting Started with MTConnect: Monitoring Your Shop Floor – What’s In It For You?” AMT - The Association for Manufacturing Technology. http://www.mtconnect.org/media/39437/gettingstartedwithmtconnectshopfloormonitoringwhatsinitforyourevapril4th-2013.pdf. [Accessed February 2, 2015].

Andradóttir, S. 1998. *Handbook of Simulation: Principles, Methodology,Advances, Applications, and Practice (Chapter 9).* New York: John Wiley & Sons.

ANSI. 2010. A*NSI/ISA-95.00.01: Enterprise-Control System Integration - Part 1: Models and Terminology*. American National Standards Institute.

Azadivar, F. 1992. “A Tutorial on Simulation Optimization.” In *Proceedings of the 1992 Winter Simulation Conference*, edited by J. J. Swain, D. Goldsmith, R. C. Crain, and J.R. Wilson, 198–204. New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Banks, J., J. S. Carson II, B.L. Nelson,, and D.M. Nicol. 2009. *Discrete-Event Simulation System*. 5th Edition, Prentice-Hall International Series in Industrial and Systems Engineering.

Better, M., F. Glover, and M. Laguna. 2007. “Advances in Analytics: Integrating Dynamic Data Mining with Simulation Optimization.” *IBM Journal of Research and Development* 51:477–488.

Bogon, T., I. J. Timm, A. D. Lattner, D. Paraskevopoulos, U. Jessen, M. Schmitz, S. Wenzel, and S. Spieckermann, 2012. “Towards Assisted Input and Output Data Analysis in Manufacturing Simulation: The EDASim Approach.” In *Proceedings of the 2012 Winter Simulation Conference*, edited by C. Laroque, J. Himmelspach, R. Pasupathy, O. Rose, and A.M. Uhrmacher, 257–269. New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Brady, T., and R. Bowden, R. 2001. “The Effectiveness of Generic Optimization Routines in Computer Simulation Languages.” In *Proceedings of the Industrial Engineering Research Conference*. Dallas, Texas.

Brady, T., and E. Yellig, E. 2005. “Simulation data mining: A New Form of Computer Simulation Output.” In *Proceedings of the 2005 Winter Simulation Conference*, edited by M. E. Kuhl, N. M. Steiger, F. B. Armstrong and J. A. Joines, 285–289. New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Carson, Y., and A. Maria. 1997. “Simulation Optimization: Methods and Applications.” In *Proceedings of the 1997 Winter Simulation Conference*, edited by S. Andradottir, K.J. Healy, D.H. Withers, and B.L. Nelson, 118–126. New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Chen, I. J. 2001. “Planning for ERP Systems: Analysis and Future Trend,” *Business Process Management Journal* 7: 374-386.

Data Mining Group (DMG). 2014. “PMML v4.2.1.” http://www.dmg.org/. [Accessed March 2, 2015].

Dudas, C., A.H.C. Hg, and H. Bostron. 2009. “Information Extraction From Solution Set Of Simulation-Based Multi-Objective Optimization Using Data Mining.” In *7th International Industrial Simulation Conference*, 65–69. Loughborough, UK.

Garcia, M., I. Roman, F. Penalvo, and M. Bonilla. 2008. “An Association Rule Mining Method for Estimating the Impact of Project Management Policies on Software Quality, Development Time and Effort.” *Expert Systems with Applications* 34: 522–529.

Gröger, C., F. Niedermann, and B. Mitschang. 2012. “Data Mining-Driven Manufacturing Process Optimization.” In *Proceedings of the World Congress on Engineering 2012 Vol III*, 4–6. London, U.K.

ISO/IEC SQL Part 1: *SQL Framework*, http://www.jtc1sc32.org/doc/N2151-2200/32N2153T-text_for_ballot-FDIS_9075-1.pdf. [Accessed July 16, 2015].

Jain, S. and G. Shao. 2014. “Virtual Factory Revisited for Manufacturing Data Analytics.” In *Proceedings of the 2014 Winter Simulation Conference*, edited by A. Tolk, S. D. Diallo, I. O. Ryzhov, L. Yilmaz, S. Buckley, and J. A. Miller, 887–898. New Jersey: Inst. of Electrical and Electronics Engineers, Inc.

Li, X., and S. Olafsson. 2005. “Discovering Dispatching Rules Using Data Mining.” *Journal of Scheduling* 8: 515–527.

MTConnect Institute, http://www.mtconnect.org. [Accessed April 3, 2015].

OAGi. *Open Application Group’s Integration Specification (OAGIS)*, Edition 10.0 .http://www.oagi.org/dnn2/DownloadsandResources/OAGIS100PublicDownload.aspx. [Accessed November 23, 2014].

Olafsson, S., X. Li, and S. Wu. 2008. “Operations Research And Data Mining.” *European Journal of Operational Research* 187: 1429–1448.

Paris, J., and H. Pierreval. 2001. “Dealing with Design Options in the Optimization of Manufacturing Systems: An Evolutionary Approach.” *International Journal of Production Research* 39: 1081–1094.

Reinhart, G., M. Gloneggera, M. Festnera, J. Egbersa, and J. Schilpa. 2012. "Adaption of Processing Times to Individual Work Capacities in Synchronized Assembly Lines Technologies and Systems for Assembly, Quality, Productivity and Customization." In *Proceedings of the 4th CIRP Conference on Assembly technologies and Systems,* edited by J. Hu. Ann Arbor, Michigan.

Remondino, M., and G. Correndo. 2005. "Data Mining Applied to Agent Based Simulation." In *Proceedings of the 19th European Conference on Modeling and Simulation.* Riga, Latvia.

Shao, G., S. Jain, and S. Shin. 2014. "Data Analytics Using Simulation for Smart Manufacturing." In *Proceedings of the 2014 Winter Simulation Conference,* edited by A. Tolk, S. D. Diallo, I. O. Ryzhov, L. Yilmaz, S. Buckley, and J. A. Miller, 2192–2203. New Jersey: Institute of Electrical and Electronics Engineers, Inc.

SISO 2012. *SISO-STD-008-01-2012: Standard for Core Manufacturing Simulation Data – XML Representation.* Simulation Interoperability Standards Organization. Orlando, F L.

Skoogh, A., Michaloski, J., and N. Bengtsson. 2010. "Towards Continuously Updated Simulation Models: Combining Automated Raw Data Collection and Automated Data Processing." In *Proceedings of the 2010 Winter Simulation Conference,* edited by B. Johansson, S. Jain, J. Montoya-Torres, and E. Yucesan, 1678–1689. New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Skormin, V.A., V.I. Gorodeski, and L.J. Popyack. 2002. "Data Mining Technology for Failure Prognostic of Avionics." *IEEE Transactions - Aerospace and Electronic Systems* 38: 388–403.

Zheng, L., C. Zeng, L. Li, Y. Jiang, W. Xue, J. Li, C. Shen, W. Zhou, H. Li, L. Tang, T. Li, B. Duan, M. Lei, and P. Wang. 2014. "Applying Data Mining Techniques to Address Critical Process Optimization Needs in Advanced Manufacturing." In *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 1739–1748.

AUTHOR BIOGRAPHIES

DEOGRATIAS KIBIRA is with Morgan State University. His current research is in developing performance assurance methodologies for smart manufacturing systems. He has PhD in Manufacturing Engineering from the University of New South Wales. His e-mail address is deogratias.kibira@.morgan.edu.

QAIS HATIM holds the Dual Degree Doctoral of Industrial Engineering and Operation Research in the Department of Industrial Engineering at The Pennsylvania State University, USA, Class of 2015. He was also a guest researcher in the Life Cycle Engineering Group in NIST's Systems Integration Division of the Engineering Laboratory. His current research is combining statistics, optimization, and data analytics with manufacturing in order to build robust models that are feasible for implementation in real life situations. His email is qaiszakry@gmail.com.

GUODONG SHAO is a computer scientist in the Life Cycle Engineering Group in NIST's Systems Integration Division of the Engineering Laboratory. His current research topics include modeling, simulation, and analysis; data analytics; and optimization for Smart Manufacturing. He served as a member of the WSC Board of Directors and on the editorial board of the International Journal on Advances in Systems and Measurements. He holds a PhD in IT from George Mason University. His email address is gshao@nist.gov.

SOUNDAR KUMARA is a Professor in Industrial and Manufacturing Engineering Department at Penn State University where he also holds a joint appointment in the School of Information Sciences and technology and the Department of Computer Science and Engineering. His email is skumara@psu.edu.

Inspection of embedded internal features in additively manufactured metal parts using metrological x-ray computed tomography

Felix H. Kim[1], Herminso Villarraga-Gómez[2], and Shawn P. Moylan[1]
[1]Production Systems Group
[1]National Institute of Standards and Technology
Gaithersburg, MD, USA
[2]X-Ray/CT Group
Nikon Metrology, Inc.
Brighton, MI, USA

INTRODUCTION

Advances in metal additive manufacturing (AM) have made it possible to build parts with complex geometry. Metal AM has a high potential to impact various industries including aerospace and automotive. Complex interior features can be designed to reduce weight and improve mechanical or thermal efficiency of the components. These features, however, are generally inaccessible from the outside to vision-based inspection techniques for quality control. Undesirable interior defects such as porosity and cracks can be formed due to sub-optimal processing parameters, poor feed stock material quality, or environmental effects [1-3]. The mission-critical structural components require thorough inspections for defects and dimensional accuracies.

X-ray Computed Tomography (XCT) – based inspection is becoming a viable option for several manufacturing industries. XCT shows a clear three-dimensional (3D) internal structure of the part in inspection. XCT has been popularly used to understand materials structure and behavior [e.g., 4, 5]. As the technique is applied to industrial inspection settings, guidelines must be established prior to widespread adoption of the technique.

To establish XCT as a reliable non-destructive evaluation tool for inspections of fracture-critical components, it is important to determine the base-line detectability of AM defect types and sizes using XCT. Probability of Detection (PoD) is a measure used to determine the capability of a non-destructive evaluation (NDE) technique. There are yet undetermined aspects of PoD and minimum detectable flaw size for typical flaws found in AM-produced parts using XCT. Only a handful of papers related to this topic have been published to date [6]. One of the critical steps in evaluating non-destructive inspection techniques including XCT will be the ability to test parts with intentionally placed simulated flaws inside AM-produced parts. Reliable artifacts with internal features that are representative of the defects occurring in AM need to be developed. Building an internal structure, however, is difficult with any conventional technique. AM, on the other hand, provides an opportunity to embed complex internal structures.

In this paper, an approach to build internal features using AM and to inspect the results using XCT are presented. Three test parts incorporating different internal features were built by a laser-based powder bed fusion (PBF) process. The qualities of these builds were determined from XCT scans. Metrological XCT scans measured the size of the internal features more accurately. The interior features were directly compared with the relevant computer-aided design (CAD) models. Based on the results, an improved artifact design is proposed.

LASER-BASED POWDER BED FUSION ADDITIVE MANUFACTURING OF SAMPLES WITH INTERNAL FEATURES

The parts were produced using laser-based PBF AM processes with a system (EOS M270) available at the National Institute of Standards

[i] Official contribution of the National Institute of Standards and Technology (NIST); not subject to copyright in the United States. The full descriptions of the procedures used in this paper require the identification of certain commercial products. The inclusion of such information should in no way be construed as indicating that such products are endorsed by NIST or are recommended by NIST or that they are necessarily the best materials, instruments, software or suppliers for the purposes described.

Kim, Felix; Villarraga-Gomez, Herminso; Moylan, Shawn.
"Inspection of embedded internal features in additively manufactured metal parts using
metrological x-ray computed tomography."
Paper presented at the American Society for Precision Engineering Summer Topical Meeting, Raleigh, NC, Jun 27-Jun 30, 2016.

and Technology (NIST). Nickel-based super alloy (Inconel 625) powder (between 15 µm and 60 µm in particle size as measured by standard sieves) was used. The laser spot size is approximately 100 µm, and the default machine parameter settings were used for the material. Three samples were designed with interior features incorporating different sizes and orientations of cubes and spheres, as shown in FIGURE 1. Un-melted powders are expected to be trapped in the voids. The outer diameters of the samples are 10 mm, 6 mm, and 5 mm, respectively.

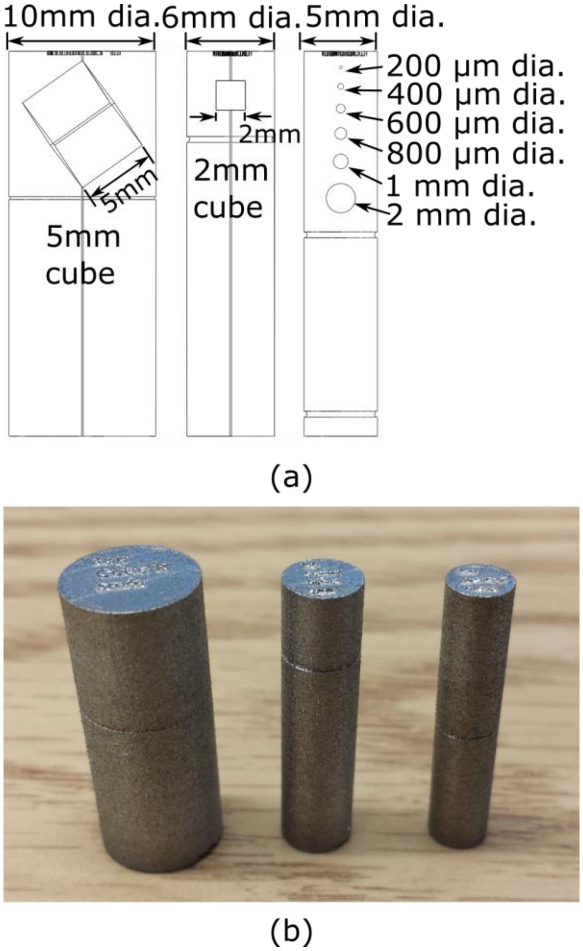


FIGURE 1. Designs of the samples with different internal features (a) and picture of the samples after the build (b).

X-RAY CT INSPECTION

Metrological XCT

Metrological XCT measurements were obtained for the three samples using an XCT system (Nikon XT H 225 ST). One of the main advantages of metrological XCT is the use of calibrated voxel size. Typical XCT techniques estimate voxel size based on magnification factor alone. However, there is potential for dimensional errors with this approach due to axis position errors, geometric alignment error of CT system hardware, and X-ray focal spot drift error. Further, image quality can be affected by physical factors such as beam hardening and the scattering of X-rays, which need to be either prevented by hardware filtering or compensated with post-processing corrections after CT reconstruction.

For the current measurement, a calibration of the voxel size and a beam hardening correction were performed. The voxel size calibration is achieved in a similar fashion to the guidelines from [7] by running a CT scan of a calibration object (FIGURE 2) with the identical scan settings to those used in measuring the test pieces. The calibration object is a hollow aluminum cylinder, which was measured with a coordinate measurement machine (CMM) to obtain reference dimensions. The XCT scan parameters are shown in *TABLE 1.* Slight differences between the effective voxel size calculated based on uncalibrated geometric magnification and the calibrated voxel size are noticed.

For CT measurements, the samples were mounted at an angle of 20º from the vertical axis to avoid cone-beam artifacts.

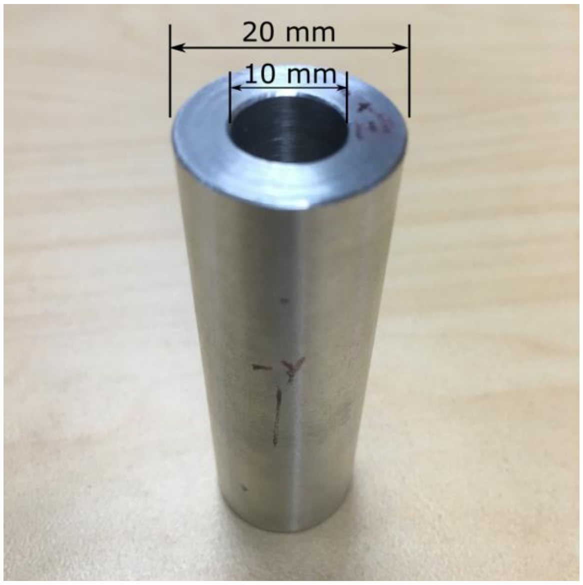


FIGURE 2. XCT calibration object

TABLE 1. XCT scan parameters

Sample	Large Cube	Small Cube	Sphere
Voltage (kV)	200	180	180
Current (µA)	91	90	90
Power (W)	18.2	16.2	16.2
Filter Type and Thickness	Copper 3 mm	Copper 3 mm	Copper 3mm
Exposure Time (ms)	1000	1000	1000
Number of Projections	2880	2880	2880
Frame Per Projection	1	1	1
Detector Pixel Size (µm)	200	200	200
Geometric Magnification	14.29	15.32	15.32
Magnification-based Voxel Size (µm)	14.00	13.06	13.06
Calibrated Voxel Size (µm)	14.05	13.08	13.08
Percent Difference (%)	0.36	0.15	0.15

Feasibility of Building Internal Features

Vertical interior slices at about the midsection of each sample are shown in FIGURE 3. High contrast of the solid parts was achieved, and the voids filled with powders can be easily distinguished from the solidified structure. The powder-trapping void looks darker due to porosity and the fairly coarse spatial resolution compared to the powder size.

In the sphere sample, the 200 µm diameter spherical pore was not built. At the current XCT spatial resolution, no visible pore is found in the area. Both the spheres and the small cube experienced difficulties with producing accurate top surfaces. On the other hand, the large cube was built relatively well despite the larger overall dimensions. Small (100 µm dia.) holes were designed and incorporated for the purpose of possibly getting the powders out, but they also did not appear to be built. Unintentional pores were not visible in the XCT images at the spatial resolution used, which confirms that the AM processing parameters used were optimal to reduce porosity formation.

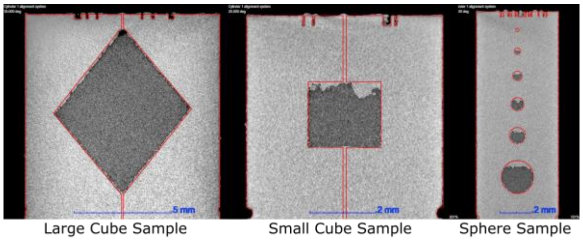


FIGURE 3. Results of metrological XCT scans and CAD overlaid.

Nominal to Actual Comparison

The metrological XCT images were directly compared to the CAD drawings as shown in FIGURE 4, 5, and 6. The XCT surface was registered to CAD via an iterative best-fit algorithm. The nominal geometry locations were subtracted from the actual position in the surfaces determined from XCT volumes. The deviations from the nominal geometry were as large as about ± 100 µm, and the locations with deviations larger than ± 50 µm are highlighted as red and magenta in the inner figures.

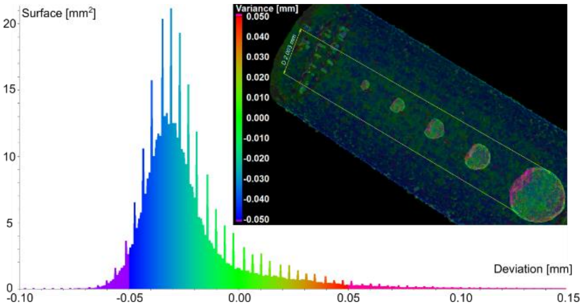


FIGURE 4. Part-to-CAD comparison showing the variance distribution for deviations of the CAD model for the sphere sample.

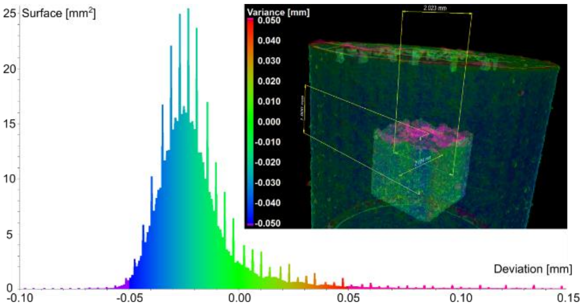


FIGURE 5. Part-to-CAD comparison showing the variance distribution for deviations of the CAD model for the small cube sample.

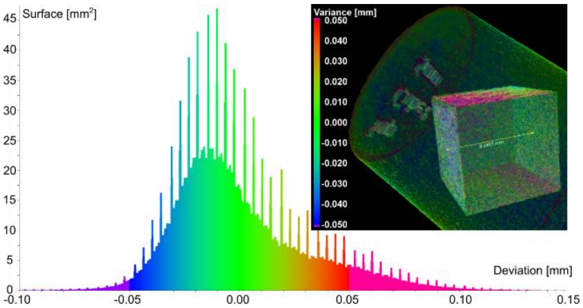


FIGURE 6. Part-to-CAD comparison showing the variance distribution for deviations of the CAD model for the large cube sample.

The nominal and actual volumes of the internal features are compared in TABLE 2. The difference between the nominal and actual volumes increased as the interior feature size decreased. The actual volumes were always smaller than the nominal volumes for the chosen designs due to inaccurate production of the top surfaces.

TABLE 2. Nominal and actual volumes of voids

	Nominal (mm^3)	Actual (mm^3)	Difference (%)
Large Cube	125	122.064	2.349
Small Cube	8	7.282	8.975
Sphere (2 mm dia.)	4.189	3.628	13.388
Sphere (1 mm dia.)	0.524	0.417	20.359
Sphere (0.8 mm dia.)	0.268	0.199	25.769
Sphere (0.6 mm dia.)	0.113	0.078	31.033
Sphere (0.4 mm dia.)	0.034	0.017	49.269

Improved Design

Based on the XCT images of the initial prototypes, an improved design is proposed to be built as an artifact for determining PoD, and an example design is shown in FIGURE 7. The design involves cubes of different sizes that are in rotated orientations. The cubes in this orientation are expected to be built closer to the nominal designs. Subsequent XCT measurements are planned for the new design.

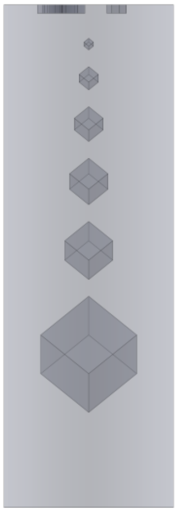


FIGURE 7. An improved design of test artifact

CONCLUSIONS

Samples incorporating internal features were built, and metrological XCT scans were obtained for the samples. The XCT scans were aligned with nominal CAD drawings for a direct comparison. Deviations up to ± 0.1 mm were detected between the nominal and measured dimensions of the AM-produced parts using XCT. Typical uncertainties of the CT measurements are in the order of 10 µm, which is a factor of five smaller than the measured deviation. Therefore, the ± 50 µm-tolerances are predominantly related to the AM process rather than the measurement uncertainty.

XCT has the ability to generate geometric data for characterization of material structures (internal and external features) and detect manufacturing defects and dimensional deviations from CAD design. To study complex structures produced by the additive manufacturing process, XCT is becoming a viable option to extract component dimensions of inner or hidden structures in a non-destructive manner. The XCT measurements also provided insights on building and embedding internal features using metal PBF processes. The metrological XCT of the controlled specimens provides good base-line data for measuring internal features. The obtained results can ultimately be used to quantitatively determine detectability of internal features using XCT.

Future plans include obtaining additional XCT images from different XCT systems for a comparison. Once all XCT scans are completed, a destructive measurement will be performed.

ACKNOWLEDGEMENTS

The authors would like to thank Mr. Mike McGlauflin of NIST for providing advice on developing a sample design, and Dr. Jarred Heigel of NIST for producing the parts with additive manufacturing.

REFERENCES

[1] Ng GKL, Jarfors AEW, Bi G, Zheng HY. Porosity formation and gas bubble retention in laser metal deposition. Appl Phys A. 2009;97:641-9.
[2] Thijs L, Verhaeghe F, Craeghs T, Humbeeck JV, Kruth J-P. A study of the microstructural evolution during selective laser melting of Ti–6Al–4V. Acta Mater. 2010;58:3303-12.
[3] Yadroitsev I, Thivillon L, Bertrand P, Smurov I. Strategy of manufacturing components with designed internal structure by selective laser melting of metallic powder. Appl Surf Sci. 2007;254:980-3.
[4] Maire E, Withers PJ. Quantitative X-ray tomography. Int Mater Rev. 2014;59:1-43.
[5] Withers PJ, Preuss M. Fatigue and Damage in Structural Materials Studied by X-Ray Tomography. Annual Review of Materials Research. 2012;42:81-103.
[6] Amrhein S, Rauer M, Kaloudis M. Characterization of Computer Tomography Scanners Using the Probability of Detection Method. JNE. 2014;33:643-50.
[7] Lifton JJ, Malcolm AA, McBride JW, Cross KJ. The Application of Voxel Size Correction in X-ray Computed Tomography for Dimensional Metrology. 2nd Singapore International Non-destructive Testing Conference & Exhibition. Marina Bay Sands, Singapore2013.

Testing of cementitious materials using a dynamic MEMS micro rheometer

Yong-Sik Kim[1], Nicholas G. Dagalakis[1], Chiara Ferraris[1], and Nicos S. Martys[1]

[1]National Institute of Standards and Technology

Abstract Incompatibility of cementitious materials with admixtures often requires time consuming testing. Usually, several mixtures need to be prepared either using concrete or paste to determine the optimum High Range Water Reducer Admixture (HRWRA) dosage and type. The number of tests increases if the dosages of supplementary cementitious materials (SCMs) are also being optimized. To help reduce testing time and amount of materials used, a high-throughput micro rheometer is being designed that is based on an oscillatory parallel plate type rheometer. This novel device is a planar single-Degree of Freedom (DOF) motion stage based on Micro Electro Mechanical Systems (MEMS) fabrication methods. To meet the requirements for application to cement-based materials, a single-DOF motion stage is driven by an electro-thermal actuator that is designed to provide a shear stress of up to 60 Pa. The device is small and inexpensive to manufacture and several of them can be used in parallel to test various mixtures of paste at the same time. A vision sensor recognizes a set of predetermined patterns embedded on the motion stages for monitoring their motions. Data were obtained on a prototype by measuring the rheological properties of bentonite.

Keywords: rheology, cement paste, MEMS, motion stage

Introduction

Satisfactory performance of the concrete used in infrastructure depends on proper placement of, and thus a clear knowledge of, the concrete flow, i.e., workability [1]. The rheology of the cement paste is one of the major controlling factors for ensuring a proper workability of the concrete. The rheological property of the cement paste can widely vary depending on the composition, including the supplementary materials used, the chemical admixtures, and the water content [2]. For the optimization process of the performance of the concrete, multiple tests with different mixtures need to be run, requiring a considerable amount of test materials, at least a few mL level volumes for a test, if using expensive conventional rotational

Kim, Yong Sik; Dagalakis, Nicholas; Ferraris, Chiara; Martys, Nicos S.
“Testing of Cementitious Materials Using a Dynamic MEMS Micro Rheometer.”
Paper presented at the 8th International RILEM Symposium in Self-Compacting Concrete- PRO100, ed., Washington, DC, May 15-May 18, 2016.

rheometers. Thus a fast and inexpensive measurement method to determine the rheological properties of the cement paste would allow the engineer to optimize the concrete composition [2] faster with a few µL level material used.

This paper proposes a novel approach to measure the rheological properties of cement paste by developing a new Micro-Electro-Mechanical Systems (MEMS) based micro rheometer. MEMS technologies have several advantages over conventional manufacturing technologies; nano- or micro-meter level resolution and accuracy [3], inexpensive cost through mass production, and small form factor [4]. The motion stage based on these MEMS technologies is mainly used to create shearing between two parallel surfaces [5] of which one is fixed and the other oscillated linearly. This is similar to a parallel plate but there is no rotational motion.

The design specifications for this MEMS micro-rheometer took into account oscillatory tests from the literature performed with a rotational parallel plate for cementitious paste. It was found that the commonly used frequency is less than 1 Hz [6]. The gap size between the parallel plates ranges from 0.4 mm to 0.6 mm [7]. The expected storage shear modulus ranges from a few hundred Pa to 1.3 MPa [6].

The accurate measurement of the displacement of the plates in the rheometer plays an important role in determining the performance of the system. For rheological measurement, the shear stress applied to the specimen and the corresponding shear rate should be monitored at the same time. In this case, most MEMS-based sensors [8] require two additional mechanical structures to measure two properties at the same time and also need separate electric circuit boards for their post-processing. In order to avoid these additional processes and equipment, a vision-based sensor was used to monitor multiple objects at the same time. Hough transform algorithms implemented in OpenCV[1] [9] were used for the processing of the vision images.

The novel micro rheometer design consists of a thermal actuator [10], dual stages, folded beams for stage support, circular patterns for visual fiducials [11], and relevant vision software. The actuator and the folded beams are designed to generate displacements larger than 200 µm with more than 100 mN force. The dual stages implement a simple shear rheometer based on the parallel plate geometry [12]. The vision software monitors the response of the test material by measuring the displacement of the detected visual fiducials. The fabricated rheometer was tested with bentonite slurry and the test results are compared with measurements from a conventional rheometer.

Design of the micro-rheometer

[1] Certain commercial products are identified in this paper to specify the materials used and procedures employed. In no case does such identification imply endorsement or recommendation by the National Institute of Standards and Technology, nor does it indicate that the products are necessarily the best available for the purpose.

The presented MEMS-based rheometer was designed to implement the parallel plate type rheometer. From various principles for the operation of parallel plate type rheometers, a simple linear shear deformation type was selected and is shown in Fig. 1. The vibrating upper plate applies a shear stress to material located between the two plates. The corresponding reaction of the material specimen is transmitted to the stationary lower plate. By measuring the reaction force at the lower stationary plate, the viscoelastic properties of the material specimen can be calculated based on the mathematical expressions given below.

The displacement of the vibrating upper plate can be expressed with complex notation as:

$$x^* = x_0 e^{i\omega t}\ , \qquad (1)$$

where x_0 is the amplitude of the displacement of the vibrating upper plate, i is the imaginary number ($\sqrt{-1}$), ω is the angular frequency, and t is time. Assuming the presented system is a single degree-of-freedom system and consists of a mass, a spring, and a damper, the motion of the presented system can be represented [13] as:

$$m\frac{d^2x^*}{dt^2} + c\frac{dx^*}{dt} + kx^* = F^*\ , \qquad (2)$$

where m is mass, c is damping, k is the stiffness of the system, and F^* is the resulting shear force in complex notation. When the system is in steady state, a sinusoidal vibration of the upper plate results in a harmonic shear force at the stationary lower plate. This force would have the same frequency with the vibrating plate but have a phase shift. This can be expressed [14] as:

$$F^* = F_0 e^{i(\omega t + \emptyset)}\ \ , \qquad (3)$$

where F_0 is the amplitude, and $\emptyset$ is a phase shift. With the above equations, in this case, the shear strain rate can be defined [14] for small deformations, as:

$$\gamma^* = tan^{-1}\frac{x^*}{d} \approx \frac{x^*}{d}\ \ , \qquad (4)$$

where d is the physical gap between the two parallel plates as shown in Fig. 1, and x_0 should be far smaller than the gap d. The shear stress is also defined as:

$$\tau^* = \frac{F^*}{A}\ \ , \qquad (5)$$

where A is the contact area indicated in Fig. 1. The relationships from Eq. (4) and Eq. (5) provide the properties of the viscoelastic materials.

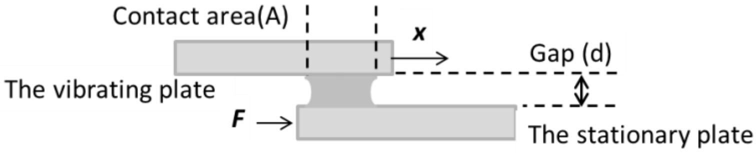


Figure 1: The parallel plates type rheometer

Most MEMS fabrication technologies are limited to monolithic or planar designs and MEMS devices are too small to handle without additional manipulators. Due to these limitations, the presented MEMS-based micro rheometer adapts the dual stage design illustrated in Fig. 2(a). The dual stage is composed of two plates: one inner plate and one outer plate. In this case, the outer stage replaces the vibrating plate and the inner stage works as the stationary plate in Fig. 1. A test specimen was placed between the inner plate and an external fixed plate. With this approach, the fabrication and handling of the presented micro rheometer becomes simple. The implementation of the conceptual design in Fig. 2(a) is described in Fig. 2(b). A thermal actuator was connected to the outer plate in order to generate oscillations that apply shear pressure to the test material specimen. The dual stages are designed by embedding one stage into the other. All movable components are supported by the folded beams to be flexible along its intended motion. The corresponding reaction force through the test specimen will move the inner plate. By measuring the displacement of the inner stage, the force transferred through the test specimen is measurable. With the force data and the vibration motion data collected at a certain vibration period, the viscoelastic material properties of a material specimen can be measured.

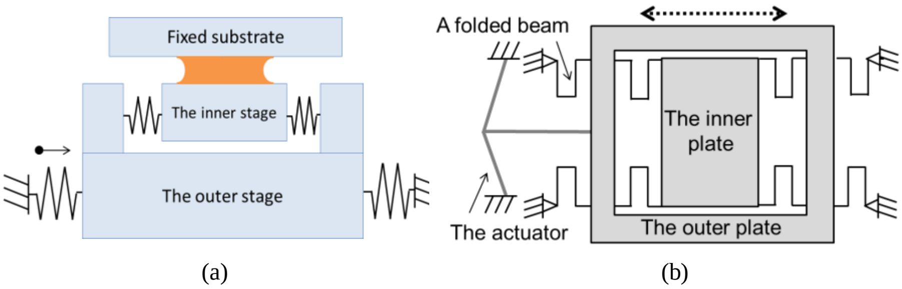


Figure 2: The implementation of the parallel plates type rheometer in MEMS; (a) the conceptual design; (b) the expected implementation of the design in (a)

Analysis of the micro rheometer

The folded beam

A folded beam supports both the inner and the outer plates and is shown in Fig. 2(b). With the analytic equation from Wong et al [15], the calculated stiffness of the inner plate is expected to be 18.5 N/m. The result from finite element analysis (FEA) modeling described in the next section is 18.4 N/m, which indicates the difference between them is less than 0.6 %

The thermal actuator

The bent-beam type thermal actuator used in the presented rheometer was also optimized to generate a motion longer than 200 µm and a shear pressure larger than tens of Pa level for larger shear rate. Based on its bent geometry, the stiffness of the actuator K_{act} is expected to be 1648.5 N/m [16]. The force generated by the actuator F_{act} is also deduced from a beam theory [4] and expected to reach up to 314.2 mN.

The vision-based displacement sensor

The vision-based sensor was utilized to measure the displacements of the inner and the outer plates at the same time. This sensor detects predetermined patterns, or visual fiducials, embedded on MEMS objects through a microscope. The visual fiducials used in this paper are pure circles in rectangular backgrounds. The main components of the presented micro rheometer do not contain any circular or curved shapes, so the circular shape can reduce faulty or wrong recognition. By using circles with different radii, the radius of the detected circular pattern can be used to identify each detected target. At least one visual fiducial is embedded on the outer and the inner stages. The vision software is based on the Circular Hough transform algorithm [11] and OpenCV [17] library.

Finite element analysis (FEA)

Finite element analysis (FEA) [18] is utilized to characterize the presented rheometer and verify the analytic relationship described in the previous section. In the whole simulation, both ends of the actuator and four ends of the folded beams are assumed to be firmly fixed and are connected to a thermal reservoir at room temperature of 20 ℃ for thermal and structural analyses.

The stiffness of the folded beam is calculated in FEA by applying a force of 1 μN along the motion direction of the actuator to the middle of the inner stage and measuring the corresponding mechanical displacement. This displacement is 54.3 nm over the whole inner plate. This result implies that the stiffness of the inner stage is 18.394 N/m.

Table I: The design parameters of the micro rheometer

Component	Symbol	Design parameter	Dimensions
Actuator beam	W	Width	70 μm
	θ	Angle	1 °
	L	Length	6500 μm
	T	Thickness	100 μm
	n	Number of beams	14
Folded beam	L_{spring}	Link length	3300 μm
	L_s	Short link length	570 μm
	W_{spring}	Link width	35 μm
	W_s	Neck length	300 μm
The inner plate	L_p	Length	9700 μm
	W_p	Width	7800 μm

The expected maximum displacement of the micro rheometer is also calculated. This simulation is the response to the thermal excitation due to a temperature rise from 20 ℃ to 550 ℃ at the center of the thermal actuator. This is because, based on existing studies [19], 550 ˚C is the maximum endurable temperature limit of silicon. Based on this limit, the micro rheometer is expected to generate a displacement of up to 265 μm without any permanent damage. This simulation is based on thermal conduction only, so the real device may generate larger displacements than this due to other factors like thermal convection.

While the presented device generates a motion of 265 µm, the corresponding maximum von Mises stress reaches up to 210.9 MPa. Considering that the yield strength of silicon is 7 GPa, there is no mechanical failure expected from the motion generated by the temperature rise of 550 ºC.

Micro-fabrication

The MEMS-based fabrication process for the presented system was based on the Silicon-On-Insulator Multi-User Multi-Processes (SOIMUMPs) [20]. The starting wafer for this system is a Silicon-On-Insulator (SOI) that is composed of a device layer of 100 µm thick, a handle layer of 500 µm thick, and an insulation layer of 2 µm thick between in between. The fabrication process consists of one metal deposition and two etchings. The metal deposition forms the metal pads for connecting the thermal actuator to the electric power and the visual fiducials for the vision software to monitor the motion of the inner and the outer plates. The first etching process generates the frontal structures including the actuator and the dual stages, and the second etching builds the supporting frames on the SOI wafer handling layer. These etching processes use a deep reactive ion etching (DRIE) [21] process.

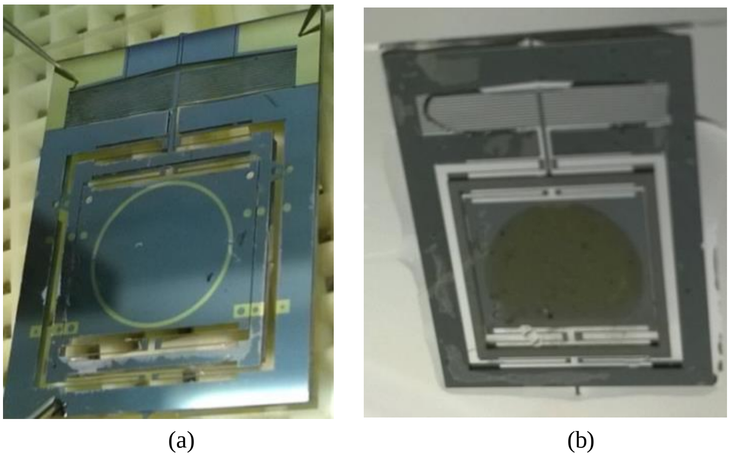

(a) (b)

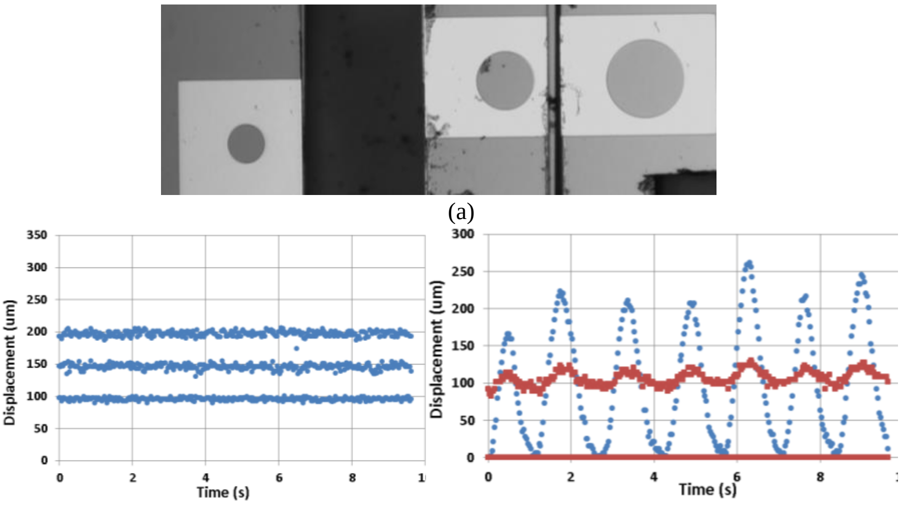
Figure 3: the microscopic images of a fabricated micro rheometer; (a) the frontal full view, (b) the backside view.

The fabricated micro rheometer is shown in Fig. 3; the shiny yellow areas in Fig. 3(a) are electric pads for the actuator and the visual fiducials for the vision software. A test specimen is placed between the micro rheometer inner plate and a transparent glass slide forming a fixed substrate as shown in Fig. 3(b).

Experimental results

The performance of the presented micro rheometer was experimentally tested and characterized. A direct current (DC) power supply unit (Agilent[1] Model 3322A[1]) was utilized to control the actuator. The visual fiducials on the micro rheometer were monitored with a PointGrey Universal Serial Bus (USB) 3.0 type Grasshopper3[1] camera through an optical microscope with a magnification ratio from 2:1 to 3:1. The camera recorded the motion of the micro rheometer during the experiment and then the vision software analyzed the captured images.

Figure 4(a) shows the visual fiducials embedded on the micro rheometer: the circular shapes inside a rectangular background. Once the vision software detects a visual fiducial, it returns the 2D position information of the detected circle and its radius. The detected radius information is plotted in Fig. 4(b); three circles with a radius of 100 µm, 150 µm, and 200 µm are well recognized without considerable noise. The radius information is utilized to identify the inner and the outer plates. Based on these results, the 2D position information is classified for the inner and the outer plates and plotted in Fig. 4(c) for 10 s. Figure 4(c) shows that three visual fiducials are correctly monitored and identified for subsequent data analysis.



(a)

(b) (c)

Figure 4: Detection of the visual fiducials: (a) the three circular patterns with rectangular backgrounds (the left one is on the inner stage, the middle one is on the outer stage, and the right one is on an outside fixture); (b) the detected radii of the patterns in (a); (c) the motion measured with the patterns in (a);

The presented micro rheometer was tested with a material test specimen: bentonite [22]. A bentonite sample with the volume of 10 µL is placed between the inner plate and an external fixed substrate. After connecting electric power to the actuator, the rheological properties of the bentonite are measured by actuating the outer plate.

The mechanical responses of the outer and the inner stages are monitored for 10 s and plotted in Fig. 5; the displacements of the inner and the outer plates are shown in red and blue lines, respectively. Figure 5 shows the amplitude difference and phase shift between the two plates. Preliminary analysis indicates that the maximum shear stress is about 40 Pa for the shear rate of about 1 s^{-1}. Tests with the same material and a rotational parallel plate rheometer have measured a shear stress of approximately 35 Pa at the same shear rate. This comparison shows that the presented micro rheometer has the potential to measure the viscoelastic properties of paste-like materials.

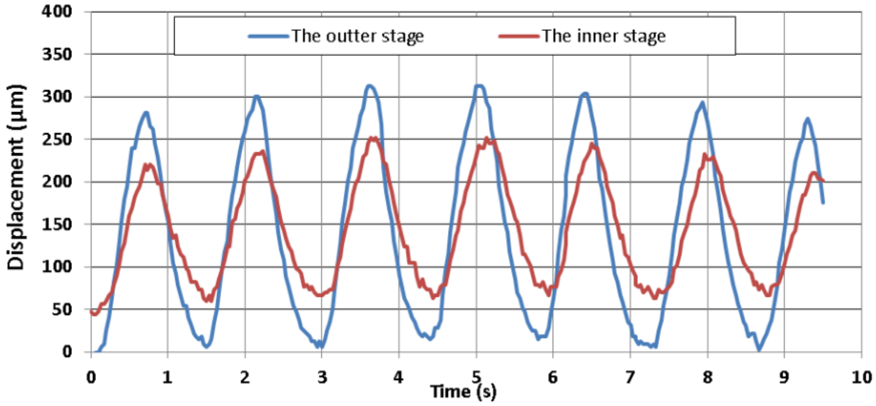


Figure 5: The measured displacements of the outer plate and the inner plate in the presented micro rheometer with a volume of 10 µL bentonite

Summary

The design, analysis, and fabrication of a MEMS-based micro rheometer have been presented for bentonite rheological measurements. In order to implement a simple shear type rheometer in MEMS, the dual stage planar micro positioner design is adapted. The dual stage is composed of one outer plate and one inner plate. The outer plate applies shear pressure to a material specimen as a vibrating plate, and the inner stage measures the force transmitted through the material specimen with respect to a stationary plate. The motions of the two plates are monitored with circular visual fiducials and a vision system with software capable to extract the desired rheological parameters.

The presented micro rheometer achieves a displacement of 300 µm for a shear rate of 1 s^{-1} to 3 s^{-1}. This micro rheometer is expected to generate a force larger than 300 mN. The rheological properties of bentonite were measured with the presented micro rheometer. The relationship between the shear stress and the shear rate generated by the micro rheometer shows similar values with those from a commercial rheometer and the relationship between viscosity and the shear rate shows a linear relationship on logarithm scale. These comparisons imply that the presented micro rheometer has a potential to provide performance similar to conventional rheometers.

The presented micro rheometer has micro-meter level resolution and needs only a few micro liter level volumes for the each test. However, the deformation on this instrument is small and not designed to simulate placement of concrete. Instead, the proposed device could be used to rapidly optimize paste composition, i.e., High Range Water Reducer Admixtures (HRWRA) or chemical admixtures dosage, incompatibility, influence of supplementary cementation materials. Also, multiple tests (5 to 10 samples) could be performed simultaneously in a disposable rheometer (no cleaning necessary.

Acknowledgement

The authors would like to thank Michelle Helsel and Lauren Martys in the Materials and Structural Systems Division at National Institute of Standards and Technology (NIST) for their support on the testing of bentonite. This research was performed in part at the NIST Center for Nanoscale Science and Technology (CNST) Nano Fabrication Clean Room.

References

[1] Lynne Brower and Ferraris, Chiara F., “Comparison of Concrete Rheometers: International Tests,” *Concr. Int.*, pp. 41 – 47, Aug. 2003.

[2] S. Jarny, N. Roussel, S. Rodts, F. Bertrand, R. Le Roy, and P. Coussot, “Rheological behavior of cement pastes from MRI velocimetry,” *Cem. Concr. Res.*, vol. 35, no. 10, pp. 1873–1881, Oct. 2005.

[3] M. J. Madou, “Fundamentals of microfabrication. 2002,” *Boca Raton Fla. CRC Press*, vol. 200, pp. 298–205.

[4] Y.-S. Kim, J.-M. Yoo, S. H. Yang, Y. M. Choi, N. G. Dagalaks, and S. K. Gupta, “Design, fabrication and testing of a serial kinematic MEMS XY stage for multifinger manipulation,” *J. Micromechanics Microengineering*, vol. 22, no. 8, 2012.

[5] G. F. Christopher, J. M. Yoo, N. Dagalakis, S. D. Hudson, and K. B. Migler, “Development of a MEMS based dynamic rheometer,” *Lab. Chip*, vol. 10, no. 20, pp. 2749–2757, 2010.

[6] Z. Sun, T. Voigt, and S. P. Shah, “Rheometric and ultrasonic investigations of viscoelastic properties of fresh Portland cement pastes,” *Cem. Concr. Res.*, vol. 36, no. 2, pp. 278–287, 2006.

[7] Ferraris, C.F., Li, Z., Zhang, M-H., “Development of a Reference Material for the Calibration of Cement Paste Rheometers,” *Accept. Publ. ASTM-Adv. Civ. Eng. Mater.*, Jun. 2012.

[8] L. L. Chu and Y. B. Gianchandani, “A micromachined 2D positioner with electrothermal actuation and sub-nanometer capacitive sensing,” *J. Micromechanics Microengineering*, vol. 13, no. 2, p. 279, 2003.

[9] R. Laganière, *OpenCV 2 Computer Vision Application Programming Cookbook: Over 50 Recipes to Master this Library of Programming Functions for Real-time Computer Vision*. Packt Publishing Ltd, 2011.

[10] L. Que, J.-S. Park, and Y. B. Gianchandani, "Bent-beam electrothermal actuators-Part I: Single beam and cascaded devices," *Microelectromechanical Syst. J. Of*, vol. 10, no. 2, pp. 247–254, 2001.

[11] "IEEE Xplore Abstract - A new concentric circle detection method based on Hough transform." on http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6295182.

[12] R. W. Chan and M. L. Rodriguez, "A simple-shear rheometer for linear viscoelastic characterization of vocal fold tissues at phonatory frequencies," *J. Acoust. Soc. Am.*, vol. 124, no. 2, pp. 1207–1219, 2008.

[13] R. W. Chan and I. R. Titze, "Viscoelastic shear properties of human vocal fold mucosa: Measurement methodology and empirical results," *J. Acoust. Soc. Am.*, vol. 106, no. 4, pp. 2008–2021, Oct. 1999.

[14] R. W. Chan and I. R. Titze, "Viscoelastic shear properties of human vocal fold mucosa: Theoretical characterization based on constitutive modeling," *J. Acoust. Soc. Am.*, vol. 107, no. 1, pp. 565–580, Jan. 2000.

[15] W. C. Wong, I. A. Azid, and B. Y. Majlis, "Theoretical Analysis of Stiffness Constant and Effective Mass for a Round-Folded Beam in MEMS Accelerometer," *Stroj. Vestn. - J. Mech. Eng.*, vol. 57, no. 6, pp. 517–525, Jun. 2011.

[16] Y. Zhu, A. Corigliano, and H. D. Espinosa, "A thermal actuator for nanoscale in situ microscopy testing: design and characterization," *J. Micromechanics Microengineering*, vol. 16, no. 2, p. 242, 2006.

[17] G. Bradski and A. Kaehler, *Learning OpenCV: Computer vision with the OpenCV library*. O'Reilly Media, Inc., 2008.

[18] A. Fluent, "12.0 User's Guide," *User Inputs Porous Media*, p. 6, 2009.

[19] M. S. Baker, J. A. Walraven, T. J. Headley, and R. A. Plass, *Final Report: Compliant Thermo-mechanical MEMS Actuators, LDRD# 52553*. United States. Department of Energy, 2004.

[20] K. Miller, A. Cowen, G. Hames, and B. Hardy, "SOIMUMPs design handbook," *MEMScAP Inc Durh.*, 2004.

[21] "Bosch DRIE process." US patent 5501893

[22] "Bentonite - Bentonite Performance Minerals, LLC." [Online]. Available: http://www.bentonite.com/bpm/default.page.

Estimating *t*-way Fault Profile Evolution During Testing

D. Richard Kuhn[1], Raghu N. Kacker[1], Yu Lei[2]

[1]*National Institute of*
Standards and Technology
Gaithersburg, MD 20899, USA
{kuhn,raghu.kacker}@nist.gov

[2]*Computer Science & Engineering*
University of Texas at Arlington
Arlington, TX, USA
ylei@uta.edu

***Abstract*: Empirical studies have shown that most software interaction faults involve one or two variables interacting, with progressively fewer triggered by three or more, and no failure has been reported involving more than six variables interacting. This paper introduces a hypothesis for the origin of this distribution, with implications for removal of interaction faults and reliability growth.**

Keywords – combinatorial testing; software fault; testing

I. Introduction

Empirical studies have shown that software interaction faults involve 1 to 6 variables, with no failures involving more than six reported. Interaction faults are denoted as *t*-way faults when *t* factors or variables induce the fault. For example, if a fault occurs when $x > 10$ *and* $y < 55$, this is a 2-way fault. Table 1 and Fig. 1 show the cumulative percentage of failures at different interaction *t* values, for a variety of applications, with the average indicated in Table 1 (headings keyed to references). For consistency, single factor faults are denoted 1-way faults. Thus for the various applications, the proportion of failures caused by 1-way or single factors ranged from 9% to 67%, and the proportion caused by either 1-way or 2-way faults ranged from 47% to 97%.

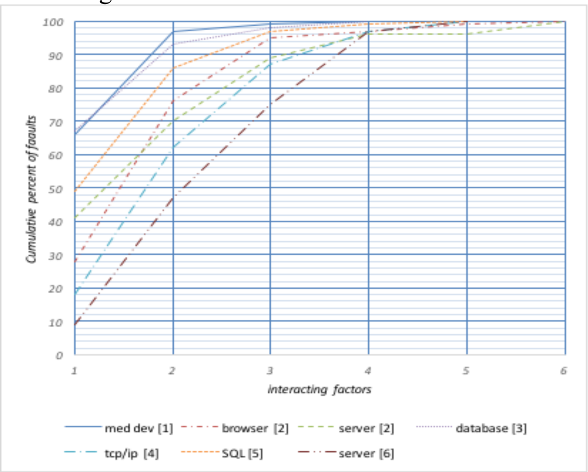
Table I. Cumulative Percent of failures at $t = 1..6$

t	[1]	[2]a	[2]b	[3]	[4]	[5]	[6]	average
1	66	28	41	67	18	9	49	39.71
2	97	76	70	93	62	47	86	75.86
3	99	95	89	98	87	75	97	91.43
4	100	97	96	100	97	97	99	98.00
5		99	96		100	100	100	99.00
6		100	100					100

The fault distributions were derived from failure reports for fielded software products, including medical devices [1], browser [2]a and server [2]b, TCP/IP [4], server [5], and SQL [6]. An additional distribution is from initial testing of a large distributed database application [3]. Empirically derived fault distributions such as these have provided the rationale for advances in the field of combinatorial testing over the past decade. While the distributions have been documented and analyzed thoroughly, relatively little is known about why the distributions have this consistent form or how they evolve as systems are tested and used. While it seems natural for more complex faults to be less common than simpler faults, we want to go beyond such a simple qualitative hypothesis and develop a model for estimating how the proportion of *t*-way faults varies with *t*, as testing or use progresses. We propose an explanation based on the two assumptions below.

- *t*-way faults occur in proportion to *t*-way conditions in code
- *t*-way faults are removed in proportion to *t*-way combinations in inputs

Fig. 1. Distribution of failures at $t = 1..6$



II. Analysis

For an estimate of the proportion of *t*-way conditions in code, we use the distribution of conditions in a collection of 7,685 branching statements from four avionics applications [7]. Note from Table II that this distribution is relatively close to the distribution of t-way faults discovered in initial testing in a database system described in reference [3].

Table II. *t*-way conditions, branch statements vs. Initial Test

t:	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
Branch cond %	74.1	19.6	4.5	1.2	.3	.1	.1	.1
Initial test [3]	67	26	5	2	0	0	0	0

As software is tested or used, interaction faults will be discovered when a *t*-way combination that triggers a fault occurs in a set of inputs. Each set of inputs includes $C(n,t)$ combinations at each level of *t*, for *n* variables, where $C(n,t) = n!/t!(n-t)!$. For variables with *v* values each, the total number of combination settings is $v^t \times C(n,t)$, so each test or input set can cover $1/v^t$ of the total number of settings. The number of values, *v*, must of course be at least 2, but may be larger. As *t* increases, the proportion of combinations covered in each test is reduced, i.e., the proportion of $(t+1)$-way

Kuhn, David; Kacker, Raghu; Yu, Lei.
"Estimating t-way Fault Profile Evolution During Testing."
Paper presented at the IEEE Conference on Computers, Software & Applications, Atlanta, GA, Jun 10-Jun 14, 2016.

combinations covered is $1/v$ of the proportion of t-way combinations covered.

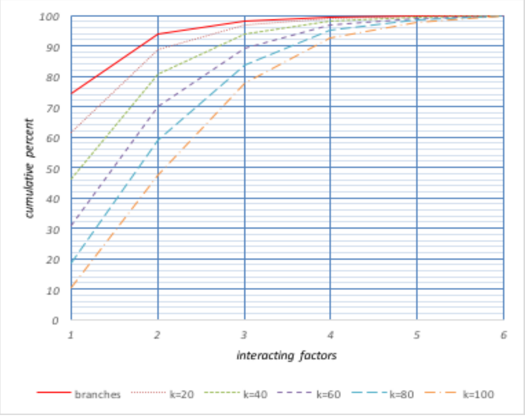
We make the simplifying assumption that 1-way faults are removed at rate r for some number of test sets, and the proportion remaining after k sets will be $(1–r)^k$. Since the discovery of a t-way fault depends on the presence of t-way combinations in input, and the proportion of $(t+1)$-way faults is $1/v$ of t-way faults, the fault discovery rate will be reduced by this proportion, or r/v for 2-way, r/v^2 for 3-way, etc. We can consider 2 the minimum value of v, and boolean or binary variables are also extremely common in practice. Then for k test sets we would have $(1 – r)^k$ 1-way faults remaining, $(1 – r/2)^k$ 2-way faults, $(1 – r/4)^k$ 3-way faults, and so on.

Now consider the evolution of the fault distribution as tests are run. Table III shows an example starting from the assumption that t-way faults occur approximately in proportion to the occurrence of t-way conditions in branching statements. For a fault detection rate of $r = .05$ per test set, $k = 48$ sets will produce a nearly matching value for the proportion of 1-way faults in the average of Table I. But the distribution of faults for $t = 2..6$ is also quite close to the average, as would be predicted if these faults are removed in proportion to $r/2$, $r/4$, $r/8$ etc. For example, starting with 74.1 1-way faults, after 48 test blocks, we would have $74.1(1 - .05)^{48} = 6.3$ 1-way faults; $19.6(1 - .05/2)^{48} = 5.8$ 2-way faults, $4.5(1 - .05/4)^{48}$ 3-way faults, etc. Normalizing this to 100%, we have the distribution shown in Table III, line (2), which is quite close to the average (3).

TABLE III. FAULTS REMAINING AT $t = 1..6$ AFTER 48 SETS OF TESTS, $r = .05$

t:	1	2	3	4	5	6+
Orig distrib %	74.1	19.6	4.5	1.2	0.3	0.3
After 48 sets	39.9	36.7	15.6	5.6	1.6	0.6
Avg, Tbl 1	39.7	37.6	15.5	6.6	1.0	1.0

FIG. 3. FAULT DISTRIBUTION FOR $t = 1..6$ AS TESTING PROGRESSES.



Notice that in Table III, after 48 test sets the proportion of faults for lower levels of t declines, while the proportion for higher t increases. Because an individual test contains a higher proportion of 1-way combinations than 2-way, the 1-way faults decline faster than others, and thus represent a smaller proportion of total remaining faults after testing. In general, t-way faults will decline faster than u-way faults for any $u>t$. This is consistent with intuition, as 2-way faults are in some sense "simpler" than 3-way faults, and thus likely to be found more quickly. Thus experience suggests that as testing progresses, the proportion of simpler faults should be reduced faster than more complex faults, shifting the distribution curves down at lower levels of t. This shift can be seen clearly in Fig. 3, which shows the proportion of faults at each level of t left after sets of tests for $r = .05$.

Fault reduction continues as bugs are detected in fielded products, and this process would result in different distributions of faults at each level of t, depending on how extensively a product is used. Data reported in two studies allow us to consider this model for a specific product. Both [2] and [5] report bug data for the Apache server, for two periods: 2001 – 2002 [2], and 2002 – 2006 [5], although some variation is likely introduced as versions were changed. Comparing columns [2]b and [5] in Table I, it can be seen that the proportion of less complex (lower t-way) faults is reduced over the time period, as expected. Starting from the distribution in [2], with $r = .05$ and $k = 54$ test sets, the distribution evolves as shown in Table IV.

TABLE IV. FAULTS REMAINING AT $t = 1..6$ AFTER 54 SETS OF TESTS, $r = .05$

t	1	2	3	4	5	6+
Rpt [2]	41	29	19	7	0	4
Rpt [5]	9	38	28	22	3	0
54 test sets	9.1	26.2	34.1	17.8	0	13.0

III. CONCLUSIONS AND IMPLICATIONS FOR TESTING

Preliminary results suggest that the model described in Sect. II is relatively successful in reproducing the fault distributions observed in empirical data. Additional empirical data will be needed to evaluate validity thoroughly.

The most significant implication for testing is that t-way interaction faults for $t = 4, 5, 6$ are exceedingly difficult to discover without tests specifically designed as covering arrays to include all t-way combinations at these levels.

Disclaimer: *Products may be identified in this document, but identification does not imply recommendation or endorsement by NIST, nor that the products identified are necessarily the best available for the purpose*

IV. REFERENCES

[1] D.R. Wallace, D.R. Kuhn, "Failure Modes in Medical Device Software: an Analysis of 15 Years of Recall Data", *Intl J. Reliability, Quality and Safety Engineering*, vol. 8, no. 4, 2001.

[2] Kuhn, D.R. and Reilly, M.J., An investigation of the applicability of design of experiments to software testing. *27th Annual NASA Software Engineering Workshop, 2002..* (pp. 91-95). IEEE.

[3] Kuhn, D.R., Wallace, D.R. and Gallo Jr, A.M., 2004. Software fault interactions and implications for software testing. *IEEE Trans Soft Eng,30*(6), pp.418-421.

[4] Bell, K.Z. Optimizing Effectiveness and Efficiency of Software Testing, PhD Diss, North Carolina State University, 2006.

[5] Cotroneo, D., Pietrantuono, R., Russo, S., & Trivedi, K. (2016). How do bugs surface? A comprehensive study on the characteristics of software bugs manifestation. *J.Systems and Software*, *113*, 27-43.

[6] Z. Ratliff, R.Kuhn, R. Kacker, Y.Lei, K. Trivedi, The Relationship Between Software Bug Type and Number of Factors Involved in Failures, submitted to Intl Wkshp Combinatorial Testing, 2016.

[7] Chilenski, J. J. *An investigation of three forms of the modified condition decision coverage (MCDC) criterion*. FAA. 2001.

Pseudo-exhaustive Testing of
Attribute Based Access Control Rules

D. Richard Kuhn[1], Vincent Hu[1], David F. Ferraiolo[1], Raghu N. Kacker[1], Yu Lei[2]

[1] *National Institute of*
Standards and Technology
Gaithersburg, MD 20899, USA
{*kuhn,vhu,david.ferraiolo,raghu.kacker*}*@nist.gov*

[2]*Computer Science & Engineering*
University of Texas at Arlington
Arlington, TX, USA
ylei@uta.edu

Abstract – **Access control typically requires translating policies or rules given in natural language into a form such as a programming language or decision table, which can be processed by an access control system. Once rules have been described in machine-processable form, testing is necessary to ensure that the rules are implemented correctly. This paper describes an approach based on combinatorial test methods for efficiently testing access control rules, using the structure of attribute based access control (ABAC) to detect a large class of faults without a conventional test oracle.**

Keywords- access control; attribute based access control; combinatorial testing; t-way testing; test automation

NOMENCLATURE

R_i	= antecedent of *i*th grant rule
T_j	= conjunction of attributes in a rule antecedent
k	= maximum number of attributes in any term
m	= number of grant rules
n	= number of attributes
p	= average number of attributes in terms
v	= number of attribute values for an attribute
C	= correct term within a rule antecedent
F	= faulty term within a rule antecedent
N	= number of rows in covering array
P	= policy as specified
P'	= policy as implemented

I. INTRODUCTION - ABAC

Attribute based access control (ABAC) [1] is a method of controlling authorization using rules that include a subject's *attributes*, along with attributes of system resources, and conditions in the environment. For example, a rule may allow access to a database if the subject's attributes include *employee* and *US_citizen*, where the rule for accessing a resource requires these attributes. This approach can be more flexible than traditional models such as role-based access control, because it is not necessary to develop a structure of users and resources in advance. The tradeoff for such flexibility is that it may be difficult or impossible to know, at a point in time, which users have access to which resources. ABAC policies can also be highly complex, with hundreds of attributes and a large number of rules. Although ABAC policies can be quite large, their rules have a regular structure – checking for the presence of specified sets of attribute values – that makes it possible to apply combinatorial methods to reduce the effort required for high-assurance testing. The need for testing can be especially acute in cases where the protected application is hosted by a third party, such as a cloud service provider, and the data owner cannot directly inspect the software used in the access control system.

This paper describes a method of testing for ABAC systems that is *pseudo-exhaustive*, which we define as exhaustive testing of all combinations of attribute values on which an access control decision is dependent. This approach is analogous to pseudo-exhaustive methods for testing combinational circuits [2], where the verification problem is reduced by exhaustively testing only the subset of inputs on which an output is dependent, or by partitioning the circuit and exhaustively testing each segment. To test ABAC systems [1][3], we can use the basic principle of testing only subsets of attributes on which a decision is dependent, although the partitioning is done in a different manner than for combinational circuits. The structure of the access control problem, ABAC in particular, makes it possible to apply the same principle by rendering the conditions for each *grant* in disjunctive normal form, then considering each term separately.

For an ABAC system, a rule with attributes *employment_status* and *time_of_day* might be, "If subject is an employee and the hour is between 9 am and 5 pm, then allow entry." The problem with this approach is that n boolean attributes or variables result in potentially 2^n rules. Many such rules may be included in written policy documents, and rules may include a variety of attributes. For any combination of attribute values, the system must implement rules that accurately reflect the written policy. The structure of such rules is typically as follows, where R_i are boolean conditions evaluating the values of one or more attributes:

R_1 → *grant*
R_2 → *grant*
…
R_m → *grant*
else → *deny*

which is equivalent to:

R_1 → *grant*
R_2 → *grant*
…
R_m → *grant*
$(\sim R_1)\ (\sim R_2) \ldots (\sim R_m)$ → *deny*

Example: Suppose we have an access rule as shown below:

United States Government work. Not subject to U.S. copyright.

Kuhn, David; Hu, Chung Tong; Ferraiolo, David; Kacker, Raghu; Lei, Yu.
"Pseudo-exhaustive Testing of Attribute Based Access Control Rules."
Paper presented at the IEEE International Conference on Software Testing, Verification and Validation (ICST) 2016, Chicago, IL, Apr 10-Apr 15, 2016.

```
if (a && (c && !d ||e))  grant();
else if (!a && b && !c)  grant();
else deny();
```

This code can be mapped to the following expression:

$(a(c\overline{d} + e) \rightarrow grant)$
$(\overline{a}b\overline{c} \rightarrow grant)$
$((\sim(a(c\overline{d} + e)))(\sim(\overline{a}b\overline{c})) \rightarrow deny)$

In a typical ABAC installation, the boolean literals could be conditions, such as *age>18*, or boolean attributes such as *employee*, but the structure will be as shown in the example. That is, a series of expressions specifying subsets of attribute conditions that must be true for access to be granted, followed by a default deny-access rule when none of the attribute expressions have been instantiated to *true*.

II. TESTING ABAC IMPLEMENTATIONS

Testing an ABAC system requires showing that the policy specified, *P*, is correctly implemented. The implemented policy *P'* must be shown to produce the same response as *P* for any combination of attributes used as input. That is, for input attributes $x_1,\dots,x_n$, $P'(x_1,\dots,x_n) = P(x_1,\dots,x_n)$.

1	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0
2	0	0	1	0	1	1	1	1	1	0	0	0	0	0	1
3	0	1	0	0	0	1	0	1	1	1	1	1	1	0	0
4	0	1	1	1	1	0	0	1	0	0	0	1	0	0	1
5	1	0	0	0	1	0	0	1	0	0	1	1	1	1	0
6	1	0	1	1	0	1	1	1	0	1	0	1	1	1	0
7	1	1	0	1	1	1	0	0	0	1	0	0	1	0	1
8	1	1	1	0	0	0	1	1	1	1	1	0	1	1	1
9	1	0	0	0	0	1	1	0	1	0	0	1	1	1	1
10	0	1	1	1	0	1	1	0	1	0	1	1	0	1	0
11	0	1	0	0	1	0	1	0	0	0	1	0	1	1	1
12	1	0	1	1	1	0	0	0	1	0	1	0	1	0	0
13	1	0	0	1	1	0	1	1	1	1	1	1	0	1	1
14	1	0	1	0	0	1	0	0	0	0	1	1	0	0	1
15	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0
16	0	1	1	0	1	0	0	0	1	1	0	1	1	1	1
17	1	1	0	1	0	0	1	1	1	0	0	0	0	0	0
18	0	0	0	0	1	1	1	1	1	1	1	1	1	0	0
19	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0
20	1	1	1	1	0	0	1	0	0	1	1	1	0	1	1
21	1	0	0	0	1	1	0	0	1	0	0	0	0	1	0
22	0	1	1	1	0	1	1	1	0	1	0	0	1	1	1

Figure 1. 3-way covering array of 15 boolean parameters

How should an ABAC system be tested? Confirming that access will be granted for users with the right attributes is easy: we can simply read off the attribute conditions for each *grant* expression and verify that the access control system returns an authorization in each case. The number of such tests is linear in the number of *grant* conditions. However, it is much more difficult to ensure that no invalid combination of attributes will result in authorization. With *n* boolean attributes or variables there are 2^n possible combinations of attributes. For example, it would not be unusual to have 50 boolean attributes, resulting in $2^{50} \approx 10^{15}$ combinations, but it must be shown that no combination will improperly allow access.

To make testing tractable, we take advantage of combinatorial methods [4][5]. To see the advantages of a combinatorial approach, refer to Figure 1, which shows a covering array of 15 boolean variables. A covering array is an *N* x *k* array of *N* rows and *k* variables. In every *N* x *t* subarray, each *t*-tuple occurs at least once. In software testing, each row of the covering array represents a test, with one column for each parameter that is varied in testing. Collectively, the rows of the array include every *t*-way combination of parameter values at least once. For example, Figure 1 shows a covering array that includes all 3-way combinations of binary values for 15 parameters. Each column gives the values for a particular parameter. It can be seen that any three columns in any order contain all eight possible combinations of the parameter values. Collectively, this set of tests will exercise all 3-way combinations of input values in only 22 tests, as compared with 32,768 for exhaustive coverage. The size of a *t*-way covering array of *n* variables with *v* values each is proportional to $v^t \log n$ [6][7]. For the example described in Sect. I, with five attributes and two possible decisions, there are $2^5 = 32$ possible rules. However, a covering array of all 3-way combinations contains only 12 rows. The number of variables for which all settings are guaranteed to be covered in a covering array is referred to as the *strength*; a 3-way array is of strength 3.

We will use covering arrays of attributes, in association with ABAC policies that have been converted to *k*-DNF form. *k*-DNF refers to disjunctive normal form where no term contains more than *k* literals. Recall that a *term* is a conjunction of one or more literals within the disjunction. For example, *abc* + *de* contains two terms, one with three literals and one with two, so the expression is in 3-DNF form. The covering array does not contain all possible input configurations, but it will contain all *k*-way combinations of variable values. Where an expression is in *k*-DNF, any term containing *k* literals that is resolved to true will clearly result in the full expression being evaluated to true. For example, an ABAC rule in 2-DNF form could be: "`if` *`employee`* `&&` *`US_citizen`* `||` *`auditor`* `then` *`grant`*". This rule contains one term of two attributes and one term of one attribute, so it is 2-DNF. Because a covering array of strength *k* contains every possible setting of all *k*-tuples and *i*-tuples for *i* < *k*, it contains every combination of values of any *k* literals.

Covering array generation tools, such as ACTS [5][6], make it possible to include constraints that prevent the inclusion of variable combinations that meet criteria specified in a first order logic style syntax. For example, if we are testing applications that run on various combinations of operating systems and browsers, we may include a constraint such as `'OS = "Linux" => browser != "IE"'`. Constraints are typically used in situations such as this, where certain combinations do not occur in practice, and therefore should not be included in tests. Modern constraint solvers such as Choco [8] and Z3 [9] make it possible to process very complex constraint sets, converting logic expressions into combinations that are invalid and can be screened from the final array.

Method: Let R = rule antecedents (left hand side of an implication rule such as p in $p \rightarrow q$) of one or more policy rules being tested in k-DNF, and T_i are terms (conjuncts of one or more attributes) in R. For the example included in the introduction, terms T_i of R would be $ac\overline{d}$, ae, and $\overline{a}b\overline{c}$. R is not necessarily the complete policy; it may be the set of rules associated with a particular resource that we wish to test, for example.

Positive testing: Generate a test set GTEST for which every test should produce a response of *grant*. It must be shown that for all possible inputs, where some combination of k input values matches a *grant* condition, a decision of *grant* is returned. Construct test set GTEST with one test for each term of R as follows:

$$\text{GTEST}_i = T_i \bigwedge_{j \neq i} {\sim}T_j$$

The construction ensures that each term in P is verified to independently produce a response of *grant*. Negating each term T_j, $i \neq j$, prevents masking of a fault in the presence of other combinations that would return the same result. For example, if a rule condition is $ab + cd \rightarrow grant$, inputs of 1100, 1101, 1110 could be used for testing $ab \rightarrow grant$. However, input 1111 would not detect the fault if the system ignores variable a or b, because the condition cd would cause a *grant* decision, and no other *grant* predicates would be evaluated. One such test is required for each term in a *grant* rule, so for m rules with an average of p terms each, the number of tests required is proportional to mp.

Negative testing: Generate a test set DTEST for which every test should produce a response of *deny*. It must be shown that for all possible inputs, where no combination of k input values matches a *grant* condition, a decision of *deny* is returned.

> DTEST = covering array of strength k, for the set of attributes included in R, with constraints specified by ~R.

Note that the structure of the access control rule evaluation makes it possible to use a covering array for DTEST, compressing a large number of test conditions into a few tests. Because a *deny* is issued only after all *grant* conditions have been evaluated, masking of one combination by another can only occur for DTEST when a test produces a response of *grant*. In such a case, an error has been discovered, which can be repaired before running the test set again. Since DTEST is a covering array, the number of tests will be proportional to $v^k \log n$, for v values per attribute (normally v=2 since most will be boolean conditions), and n attributes. For m rules, the number of tests is multiplied by the constant m.

Example: Table 1 gives a set of boolean attributes a through e, where each row defines values for the attributes that determine a decision, either *grant* or *deny*. Thus a covering array for the antecedent R of a rule in 3-DNF such as ($ac\overline{d} + \overline{a}b\overline{c} \rightarrow grant$) is given in Table 1. The total number of 3-way combinations covered is the number of settings of three binary variables multiplied by the number of ways of choosing three variables from five, i.e., $2^3 \binom{5}{3} = 80$.

Table 2 shows a covering array for this set of variables generated using ~ R as a constraint. That is, the two terms of the rule, $ac\overline{d}$ and $\overline{a}b\overline{c}$, have been excluded from the array, but all other 1-, 2-, and 3-way combinations can be found in the array. Because $ac\overline{d}$ and $\overline{a}b\overline{c}$ are the only conditions under which access should be granted, the array in Table 2 should result in a *deny* response from the access control system for every test. Collectively, the tests include all 78 3-way settings of attributes that will not instantiate the access control rule to *true*.

	a	b	c	d	e
1	0	0	0	0	0
2	0	0	1	1	1
3	0	1	0	1	0
4	0	1	1	0	1
5	1	0	0	1	1
6	1	0	1	0	0
7	1	1	0	0	1
8	1	1	1	1	0
9	1	1	0	0	0
10	0	0	1	1	0
11	0	0	0	0	1
12	1	1	1	1	1

Table 1. 3-way covering array

	a	**b**	**c**	**d**	**e**
1	0	0	0	0	0
2	0	0	1	1	1
3	0	1	1	0	0
4	1	0	0	1	0
5	1	0	1	1	0
6	1	1	0	0	1
7	1	1	1	1	1
8	0	0	1	0	1
9	1	1	0	1	0
10	0	0	0	1	1
11	1	0	0	0	0
12	0	1	1	1	0
13	1	0	0	0	1
14	0	1	1	0	1

Table 2. 3-way covering array with constraint ~*R*

III. Fault Detection

Now consider the faults that this method can detect. Suppose that some combination of attributes exists that produces a different response than required by the policy *P* in *k*-DNF form. Tests contained in GTEST and DTEST will detect a large class of missing terms, added terms, or altered terms containing *k* or fewer attributes. In this section we analyze faults that will be detected, and the underlying conditions in these faults. Table 3 illustrates the fault types and detection conditions for each.

	Term	**C=correct term**	**F=faulty term**	**GTEST detect condition**	**DTEST detect condition**	notes
1	**missing**	*abc*	--	*abc*	*none*	
2	**added**	--	*ab*	*none*	*ab*	
3		*abc*	$\bar{a}b$	*none*	$\bar{a}bc$, $\bar{a}b\bar{c}$	
4		*abc*	*ab*	*none*	$abc\overline{}$	
5		*ab*	*abc*	--	--	*no fault*
6	**altered**	*abc*	$ab\bar{c}$	*abc*	$ab\bar{c}$	
7		*abc*	*ab*	*none*	$abc\overline{}$	
8		*abc*	$\bar{a}b$	*abc*	$\bar{a}bc$, $\bar{a}b\bar{c}$	

Table 3. Example faults and detection conditions.

k-DNF detection property: Collectively, tests from GTEST and DTEST will detect added, deleted, or altered faults with up to *k* attributes.

Proof outline: Three cases can be considered, for missing, added, or altered terms in the policy. The analysis for each case is keyed to the numbered examples in Table 3.

Missing term. (1) Fault detected by GTEST. If a term is missing in the faulty implementation *P*', then there is some combination of attributes accepted in *P* that is not included in *P'*. Since it is in *P*, GTEST will include the combination and the fault will be detected.

Added term. If the system incorrectly issues a *grant* response, then some combination *F* of attributes accepted in *P'* is not included in *P*. We consider three cases depending on the number of attributes, *j*, in the added term.

> $j < k$ and *F* is not a subset of some other term (2, 3). Detected by DTEST because the added term will be part of the non-*grant* combinations in DTEST.
>
> $j < k$ and *F* is a subset of some other term (4). Detected by DTEST. If the *j* attributes of the added term are a subset of some term *C* in *P*, then because DTEST contains all *k*-way combinations not excluded by *R*, it will include all *k*-way combinations of the attributes in *F* with settings different from *C*. For example, if *F* = *ab* = 11, and *C* = *abc* = 110, then DTEST will include other settings of *abc*, which will include *abc* = 111. But because this term includes *F*, it will produce an incorrect grant response, detecting the fault. Note that if *P* contains both *abc* and $ab\bar{c}$, then the result of grant for *ab* = 11 is in fact correct, since $ab\bar{c} + abc = ab$.
>
> $j < k$ and there is some term *C* in *P* that is a subset of *F* (5). In this case a fault does not exist because any input that produces a *grant* response from *P* would produce a *grant* response with *F* added, because *F* contains all attributes of *C*.

Altered term. Three cases can be distinguished, based on the number of attributes *j* in the incorrect term *F* as compared with *k*.

> $j = k$ (6). Detected by GTEST because it includes a test with the correct term, and no other combination of attributes in that test will match any other term in *P*.
>
> $j < k$ and *F* is a subset of some other term (7). Detected by DTEST if there is no other term in *P*' that excludes from DTEST $F \cup x$, where *x* is one or more attributes in *C* that are not in *F*. Example: if *C* = *abc* and *F* is *ab*, then $ab\bar{c}$ is in DTEST, unless *P'* also contains $b\bar{c}$. Note that if DTEST includes $F \cup x$, because there is some other term *D* in *P* where $x \subseteq D$, then there is no fault because the disjunction of the altered term with the other term would not accept any attribute sets not accepted in *P*. Not detected by GTEST because any test that contains the attributes of the correct term *C* will contain all attributes of a subset of *C*.
>
> $j < k$ and *F* is not a subset of altered term *C* (8). Detected by GTEST because it will include *C*, and *P'* will not match *C*. □

If more than k attributes are included in the altered term, some faults are still detected.

> $j > k$ and *C* is not a subset of *F*. Detected by GTEST because *C* will be included in GTEST but will produce a deny response.
>
> $j > k$ and *C* is a subset of *F*. Not detected by DTEST because DTEST excludes *C*, and therefore excludes *F* because it contains *C*. Not necessarily detected by GTEST because the settings of attributes *x* in *F* but not *C* may result in $C \cup x = F$. This case can be resolved by strengthening the covering array DTEST, using an array of strength *k*+*i* to detect faulty terms with up to *i* additional attributes.

IV. Tradeoffs and Practical Considerations

The process scales easily to systems with a large number of attributes that must be included in access decisions. Because the number of rows in a covering array grows only with log *n* for *n* variables/attributes at a given number of attributes and values, a larger policy specification, involving many more attributes, requires only a few additional tests. For example, it is possible to cover all 3-way combinations of 100 boolean variables with 45 tests, increasing only to 57 tests for 300 variables.

The most significant limitation for this approach occurs where terms in access control rules contain a large number of attribute values per attribute. Although covering array size grows only with log *n*, the value of *k* for the *k*-DNF form of rules is an exponent in the number of combinations that must be covered, and consequently the number of rows increases with v^k, for *v* attribute values. If terms in the rules contain more than six or seven attributes, it may not be practical to generate covering arrays, given the limitations of today's algorithms. However, a large number of tests is not a barrier, because the structure of the solution resolves the oracle problem by ensuring that every test in GTEST should produce a response of *grant* and every test in DTEST should produce a response of *deny*. This means that tests can be fully automated, making it possible to execute a large number of tests.

Table 5 shows test set sizes for a variety of configurations, assuming a value of $p = 4$ terms per rule. The column *N* tests gives the size *N* of a covering array for k-way combinations of *n* attributes with *v* values each. The size of DTEST is $m \times N$, since there will be one covering array per rule tested. Note that the test time for even a large test set of more than 600,000 tests would be roughly 10 minutes, assuming a time of 1 ms per test. In addition, since the tests are independent, testing can be divided among as many processors as are available, so even millions of tests could be tractable.

k	*v*	*n*	*m*	N tests	#GTEST	#DTEST
3	2	50	20	36	80	720
			50		200	1800
		100	20	45	80	900
			50		200	2250
	4	50	20	306	80	6120
			50		200	15300
		100	20	378	80	7560
			50		200	18900
	6	50	20	1041	80	20820
			50		200	52050
		100	20	1298	80	25960
			50		200	64900
4	2	50	20	98	80	1960
			50		200	4900
		100	20	125	80	2500
			50		200	6250
	4	50	20	1821	80	36420
			50		200	91050
		100	20	2337	80	46740
			50		200	116850
	6	50	20	9393	80	187860
			50		200	469650
		100	20	12085	80	241700
			50		200	604250

Table 4. Test set sizes.

V. HIPAA PRIVACY EXAMPLE

The following text is an excerpt from Health Insurance Portability and Accountability Act (HIPAA) rules that specify when a health care organization must treat a patient's personal representative of as the individual [10]. (This policy fragment has been used in previous work on formal specification of natural language policies [11].) Typical cases include a parent making decisions on behalf of a child.

> *(g)(1) Standard: Personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.*
>
> *(2) Implementation specification: adults and emancipated minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.*
>
> *(3)(i) Implementation specification: unemancipated minors. If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:*
>
> *(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative; (B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or (C) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.*

Step 1: Review the text to identify attributes or variables that must be considered in access rules. Attributes in statutes may represent existence of various documents signed by the parties, among other basic attributes such as age, citizenship, etc. For this example, we consider the rules specified in (g)(3)(i)(A), for cases in which a minor has the authority to act as an individual. Each attribute is given a short mnemonic name in the covering array. These are shown below by bracketing each attribute, with a variable name annotation:

(A) The **{minor consents : mc}** to such health care service**;** no **{other consent : oc}** to such health care service is required by law, regardless of whether the consent of another person has also been obtained; **and** the minor has not **{requested that such person be treated as the personal representative : mr}**; (B) The **{minor may lawfully obtain : lo}** such health care service without the consent of a parent, guardian, or other person acting in loco parentis, **and** the **{minor : mc}**, a **{court : cc}**, or **{another person : oc}** authorized by law consents to such health care service; **or** (C) A **{parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality : pc}** between a covered health care provider and the minor with respect to such health care service.

Step 2: Convert the text description to rules in *k*-DNF form, in this case, 3-DNF. This mapping is as shown in Table 5. Note that the "or" connector prior to clause (C) indicates a disjunction of the three clauses.

Text	**Attributes**
(A) The **{minor consents : mc}** to such health care service**;** no **{other consent : oc}** to such health care service is required by law, regardless of whether the consent of another person has also been obtained; **and** the minor has not **{requested that such person : mr}** be treated as the personal representative;	expression: mc && ~oc && ~mr
	attribute sets: {mc, ~oc, ~mr}
(B) The **{minor may lawfully obtain : lo}** such health care service without the consent of a parent, guardian, or other person acting in loco parentis, **and** the **{minor : mc}**, a **{court : cc}**, or **{another person : oc}** authorized by law consents to such health care service;	expression: lo && (mc||cc||oc) = lo && mc || lo && cc || lo && oc
	attribute sets: {lo, mc}, {lo, cc}, {lo, oc}
(C) A **{parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality : pc}**	expression: pc
	attribute sets: {pc}

Table 5. Mapping of text to attributes.

Step 3: Determine the maximum number of *AND* connectives in access rule conditions. In the HIPAA example, three attributes are conjoined in Sect. (g)(3)(i)(A): "*minor consents ...; no other consent to such health care service is required by law, ...; and the minor has not requested that such person be treated as the personal representative*". Because the expression above is in 3-DNF, with a maximum of three attributes in conjunction, a 3-way covering array is sufficient to consider all relevant combinations of attribute values. Note that other practical cases may involve more than 3-way combinations of attributes in terms, but the process would be the same as in this illustrative example. Combining these terms, we have:

mc && ~oc && ~mr || lo && (mc || cc || oc) || pc → *grant*
=
mc && ~oc && ~mr || lo&&mc || lo&&cc || lo&&oc || pc → *grant*

Step 4:
GTEST: Generate tests for GTEST, with one test for each term and other terms false. Tests are shown in Figure 2.

	mc	oc	mr	lo	cc	pc
1	1	0	0	0	0	0
2	1	0	1	1	0	0
3	0	1	0	1	0	0
4	0	0	0	1	1	0
5	0	0	0	0	0	1

GTEST

	mc	oc	mr	lo	cc	pc
1	0	0	0	0	0	0
2	0	0	1	1	0	0
3	0	1	0	0	1	0
4	0	1	1	0	0	0
5	1	0	1	0	1	0
6	1	1	0	0	0	0
7	1	1	1	0	1	0
8	0	0	0	1	0	0
9	0	0	0	0	1	0
10	1	0	1	0	0	0
11	1	1	0	0	1	0
12	0	1	1	0	1	0

DTEST

Figure 2. Completed GTEST and DTEST arrays.

DTEST: Compute a covering array for DTEST for the value of *t* determined in Step 2, using *~R* as a constraint. For illustration purposes, we include a covering array of the six variables without constraints in Figure 3, followed by a covering array computed with the expression above as a constraint. Note that no terms from the expression above can be found in the constrained array. For example, because array (1) includes all 3-way combinations, mc && ~oc && ~mr is present, but in (2) it is not found, although all other 3-way combinations of these variables are present in the array (2).

	mc	oc	mr	lo	cc	pc
1	0	0	0	0	0	0
2	0	0	1	1	1	1
3	0	1	0	1	0	1
4	0	1	1	0	1	0
5	1	0	0	1	1	0
6	1	0	1	0	0	1
7	1	1	0	0	1	1
8	1	1	1	1	0	0
9	1	1	0	0	0	0
10	0	0	1	1	0	0
11	0	0	0	0	1	1
12	1	1	1	1	1	1

(1) Covering array
without constraint

	mc	oc	mr	lo	cc	pc
1	0	0	0	0	0	0
2	0	0	1	1	0	0
3	0	1	0	0	1	0
4	0	1	1	0	0	0
5	1	0	1	0	1	0
6	1	1	0	0	0	0
7	1	1	1	0	1	0
8	0	0	0	1	0	0
9	0	0	0	0	1	0
10	1	0	1	0	0	0
11	1	1	0	0	1	0
12	0	1	1	0	1	0

(2) Covering array
with constraint

Figure 3. DTEST array compared with unconstrained array.

VI. RELATED WORK

A variety of methods have been introduced for testing ABAC systems, particularly those implemented using the Extensible Access Control Meta Language (XACML) [12]. Xu and Zhang provide a survey of these methods [16], which have generally been based on a fault model with mutation operators, or policy coverage. Popular tools for fault model based testing include Margrave [19], which uses a specialized model checker, and has been applied to XACML policies. It has also been used as the foundation for mutation-based test generators, including a redundant rule checking tool called Cirg, which supports mutation testing tool Targen, which has been shown to produce high levels of structural coverage [17][15][18]. Another, the Access Control Policy Testing tools ACPT [20], uses the NuSMV language and model checker to support testing a broad range of policies, including ABAC, role based access control, and customized policies specified by users in the ACPT tool. ACPT includes combinatorial coverage of inputs for tests, a feature also provided by the Simple Combinatorial Test Generation algorithm and its related tools [22][23].

Pseudo-exhaustive test methods for circuit testing have an extensive history of application [2]. While our method is not derived from these earlier approaches, it shares the basic notion of determining dependencies, partitioning according to these dependencies, and testing exhaustively the inputs on which an output is dependent. We have previously applied this notion to software testing in a more general form, using the observation that faults depend on a small number of inputs, by covering all 2-way to 6-way combinations of inputs [24].

VII. CONCLUSIONS

Correct implementation of access control requires that policies written in natural language are mapped to machine-enforceable rules, and that these rules are correctly implemented. If access control rules contain at most *k* boolean attributes per conjunction, for an expression in *k*-DNF, then a *k*-way covering array includes all possible settings of such terms. Thus for any possible combination of *n* inputs, only *k*, $k < n$, matter in determining the truth of the expression. In most applications, the number of conditions will be small. The number of rows in a *k*-way covering array of boolean variables is proportional to $2^k \log n$. Thus for any given value of *k*, even a large number *n* of attributes requires only a test set proportional to log *n* to determine access for all possible inputs. The structure of the access control problem makes it possible to construct two test sets, GTEST and DTEST, for which the expected result is always *grant* or *deny* respectively. This structure eliminates the need for a conventional test oracle, so several hundred thousand tests can be generated and run automatically in a few minutes.

The HIPAA worked example included in this paper shows that this process is practical for real-world use. We plan to continue developing the approach, extending it for special cases such as priorities among rule conditions. As ABAC becomes more widely used, the method may assist developers in ensuring that policies are implemented correctly, and meet organizational requirements.

Disclaimer: *Products may be identified in this document, but identification does not imply recommendation or endorsement by NIST, nor that the products identified are necessarily the best available for the purpose.*

REFERENCES

[1] V. C. Hu et al., Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162, January 2014.

[2] McCluskey, E. J. (1984). Verification Testing: A Pseudoexhaustive Test Technique. *Computers, IEEE Transactions on*, *100*(6), 541-546.

[3] Hu, V. C., Kuhn, D. R., Xie, T., & Hwang, J. (2011). Model checking for verification of mandatory access control models and properties. *International Journal of Software Engineering and Knowledge Engineering*, *21*(01), 103-127.

[4] Kuhn, D. R., Kacker, R. N., & Lei, Y. (2010). SP 800-142. Practical Combinatorial Testing.

[5] ACTS Home Page, http:// csrc.nist.gov/acts/

[6] Y. Lei, R. Kacker, D.R. Kuhn, V. Okun, J. Lawrence, IPOG: A general strategy for t-way software testing. *14th international conference on the engineering of computer-based systems*, 2007, pp 549–556

[7] D. M. Cohen, S. R. Dalal, M. L. Fredman, and G. C. Patton, "The AETG System: An Approach toTesting Based on Combinatorial Design," *IEEE Trans. Software Eng.*, 23(7):437-444,1997.

[8] Jussien, N., Rochart, G., & Lorca, X. (2008). Choco: an open source java constraint programming library. In *CPAIOR'08 Workshop on Open-Source Software for Integer and Contraint Programming (OSSICP'08)* (pp. 1-10).

[9] De Moura, L., & Bjørner, N. (2008). Z3: An efficient SMT solver. In *Tools and Algorithms for the Construction and Analysis of Systems* (pp. 337-340). Springer Berlin Heidelberg.

[10] United States Congress. Health Insurance Portability and Accountability Act; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996

[11] H. DeYoung, D. Garg, L. Jia, D. Kaynar, and A. Datta. Experiences in the logical specification of the HIPAA and GLBA privacy laws. In Proceedings of the 9th annual ACM Workshop on Privacy in the Electronic Society (WPES), 2010. Full version: Carnegie Mellon University Technical Report CMU-CyLab-10-007.

[12] The eXtensible Access Control Markup Language (XACML), Version 3.0, OASIS Standard, January 22, 2013, <URL: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf

[13] Bertolino, A., Lonetti, F., & Marchetti, E. (2010, September). Systematic XACML request generation for testing purposes. In *Software Engineering and Advanced Applications (SEAA), 2010 36th EUROMICRO Conference on* (pp. 3-11). IEEE.

[14] Hu, V. C., Martin, E., Hwang, J., & Xie, T. (2007, July). Conformance checking of access control policies specified in XACML. In *Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International* (Vol. 2, pp. 275-280). IEEE.

[15] Martin, E., & Xie, T. (2007, May). A fault model and mutation testing of access control policies. In *Proceedings of the 16th international conference on World Wide Web* (pp. 667-676). ACM.

[16] Xu, D., & Zhang, Y. (2014, June). Specification and Analysis of Attribute-Based Access Control Policies: An Overview. In *Software*

Security and Reliability-Companion (SERE-C), 2014 IEEE Eighth International Conference on (pp. 41-49). IEEE.

[17] Martin, E. (2006, October). Automated test generation for access control policies. In *Companion to the 21st ACM SIGPLAN symposium on Object-oriented programming systems, languages, and applications* (pp. 752-753). ACM.

[18] Martin, E., & Xie, T. (2007, May). Automated test generation for access control policies via change-impact analysis. In *Proceedings of the Third International Workshop on Software Engineering for Secure Systems* (p. 5). IEEE Computer Society.

[19] Fisler, K., Krishnamurthi, S., Meyerovich, L. A., & Tschantz, M. C. (2005, May). Verification and change-impact analysis of access-control policies. In *Proceedings of the 27th international conference on Software engineering* (pp. 196-205). ACM.

[20] V. Hu, D.R. Kuhn, T. Xie, Property Verification for Generic Access Control Models, IEEE/IFIP International Symposium on Trust, Security, and Privacy for Pervasive Applications, Shanghai, China, Dec. 17-20, 2008.

[21] ACPT Home Page, http://csrc.nist.gov/groups/SNS/acpt/access_control_policy_testing.html

[22] Bertolino, A., Lonetti, F., & Marchetti, E. (2010, September). Systematic XACML request generation for testing purposes. In *Software Engineering and Advanced Applications (SEAA), 2010 36th EUROMICRO Conference on* (pp. 3-11). IEEE.

[23] Bertolino, A., Daoudagh, S., Lonetti, F., & Marchetti, E. (2012, April). Automatic XACML requests generation for policy testing. In *Software Testing, Verification and Validation (ICST), 2012 IEEE Fifth International Conference on* (pp. 842-849). IEEE.

[24] D. R. Kuhn, V. Okun, Pseudo-exhaustive Testing For Software, 30th NASA/IEEE Software Engineering Workshop, April 25-27, 2006

[25] Working DRAFT Information technology - Next Generation Access Control –Generic Operations and Data Structures (NGAC-GOADS)), INCITS 499-2013, American National Standard for Information Technology, American National Standards Institute, April 2014.

Characterization of type-II spontaneous parametric down-conversion in domain-engineered PPLN

Paulina S. Kuo[1,]*, Thomas Gerrits[2], Varun Verma[2], Sae Woo Nam[2], Oliver Slattery[1], Lijun Ma[1] and Xiao Tang[1]

[1]Information Technology Laboratory, National Institute of Standards and Technology (NIST),
100 Bureau Drive, Gaithersburg, MD, USA 20899-8920

[2]Physical Measurement Laboratory, National Institute of Standards and Technology (NIST),
325 Broadway, Boulder, CO, USA 80305-3337

ABSTRACT

We characterize spontaneous parametric downconversion in a domain-engineered, type-II periodically poled lithium niobate (PPLN) crystal using seeded emission and single-photon techniques. Using continuous-wave (CW) pumping at 775 nm wavelength, the signal and idler are at 1532.5 nm and 1567.5 nm, respectively. The domain-engineered crystal simultaneously phasematches signal and idler pairs: [H(1532.5 nm), V(1567.5 nm)] and [V(1532.5 nm), H(1567.5 nm)]. We observe the tuning curves of these processes through difference-frequency generation and through CW fiber-assisted, single-photon spectroscopy. These measurements indicate good matching in amplitude and bandwidth of the two processes and that the crystal can in principle be used effectively to generate polarization-entangled photon pairs.

Keywords: quantum optics; nonlinear optics, parametric processes; polarization entangled pair source; spontaneous parametric downconversion; entanglement

1. INTRODUCTION

Entanglement is an important resource for quantum information systems. Entangled photon pairs generated by spontaneous parametric down-conversion (SPDC)[1,2] are an important tool for distributing entanglement between different systems and across large distances. By using quasi-phasematching (QPM)[3] in an SPDC crystal, a wide variety of nonlinear interactions with different wavelengths, bandwidths and polarization states can be obtained[4–6]. Photons generated near the 1550 nm telecom wavelength are very attractive for long-distance entanglement distribution over existing fiber links[5,7–9], which is important for the realization of practical quantum information networks.

We have designed a new scheme for generating polarization-entangled photons[10,11]. It is related to schemes that use two collinear processes in two consecutive, co-rotated crystals[12,13] and schemes that use two consecutive QPM periods[7,8]. These two schemes generate photon pairs of different polarizations but matched wavelengths. There is ambiguity where the pump photon is down-converted and which signal and idler pair is generated, and this ambiguity leads to quantum entanglement. In our scheme, instead of two discrete locations in the down-conversion crystal, we use a phase-modulated structure for the QPM grating that simultaneously phasematches the two type-II SPDC processes corresponding to $|H_{sig}V_{idl}\rangle$ and $|V_{sig}H_{idl}\rangle$[10,11]. This grating was fabricated in periodically poled lithium niobate (PPLN).

We have made progress in characterizing signal and idler generation in the domain-engineered crystal, but most of the measurements used seeding with classical light. It has been shown that there is a close relationship between stimulated and spontaneous emission of photon pairs, and that examining the stimulated emission processes can be a fast and effective means to gather information about the spontaneous emission processes[14]. Our measured seeded spectra showed good spectral matching between the two orthogonally polarized SPDC processes[11]. We recently have performed single-photon characterization of spontaneous photon pairs generated in the domain-engineered QPM crystal. Measurements were performed using fiber-assisted single-photon spectroscopy[15-17]. Here, we describe results of these single-photon characterizations and discuss implications for quantum entanglement. These single-photon measurements were in agreement with seeded spectral measurements.

*pkuo@nist.gov

Advances in Photonics of Quantum Computing, Memory, and Communication IX, edited by Zameer Ul Hasan,
Philip R. Hemmer, Hwang Lee, Alan L. Migdall, Proc. of SPIE Vol. 9762, 976211
© 2016 SPIE · CCC code: 0277-786X/16/$18 · doi: 10.1117/12.2218535

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 03/21/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

2. THEORY

2.1 Engineering spontaneous parametric down-conversion

In the process of SPDC, a high-intensity pump at angular frequency ω_p incident on a second-order nonlinear optical crystal spontaneously splits into pairs of lower energy (longer wavelength) photons (signal, ω_s, and idler, ω_i) that are related to the pump photons by energy conservation ($\omega_p = \omega_s + \omega_i$). The spectrum of down-conversion is determined by

$$I_{SPDC} \propto \mathrm{sinc}^2\left(\frac{\Delta kL}{2}\right), \tag{1}$$

with sinc(x) = sin(x)/x, L is the length of the crystal, and for a collinear interaction,

$$\Delta k = k_p - k_s - k_i \pm \frac{2\pi}{\Lambda_{QPM}}, \tag{2}$$

where the wavevector $k_j = 2\pi n_j/\lambda_j$, n_j is the refractive index at wavelength λ_j and Λ_{QPM} is the period of the domain inversion pattern when quasi-phasematching is applied. Maximum conversion is obtained when $\Delta k = 0$. Since the indices of refraction depend on temperature, tuning of the wavelengths can be achieved by changing the crystal temperature.

A number of advanced techniques have been developed to modify the domain inversion pattern in order to engineer the frequency conversion spectrum. Here, we apply phase modulation of the QPM grating to produce multi-wavelength conversion[18,19]. In this technique, the domain positions within each period Λ_{QPM} are shifted with a shift characterized by a phase that ranges from 0 to 2π. The phase-shift pattern is periodic with period Λ_{ph}. If one wants to phasematch two processes with associated phase mismatches Δk_1 and Δk_2, then a phase-modulated grating can be designed such that

$$k_p - k_s - k_i = 2\pi\left(\frac{1}{\Lambda_{QPM}} + \frac{m_j}{\Lambda_{ph}}\right) = 0\,. \tag{3}$$

where m_j is the integer associated with process j (for the two-process example, j = 1 or 2). We have previously applied the phase-modulation technique to engineer dual-wavelength sum-frequency generation[20].

For type-II SPDC where we want to simultaneously generate $|\mathrm{H_{sig}V_{idl}}\rangle$ and $|\mathrm{V_{sig}H_{idl}}\rangle$, the two processes are

$$\begin{aligned} \omega_p^{\mathrm{H}} &= \omega_s^{\mathrm{V}} + \omega_i^{\mathrm{H}} \\ \omega_p^{\mathrm{H}} &= \omega_s^{\mathrm{H}} + \omega_i^{\mathrm{V}} \end{aligned}\,. \tag{4}$$

If we assign m_1= -1 and m_2 = 1, then for 776 nm → 1535 nm + 1570 nm in MgO-doped PPLN[21], we calculate the required periods are Λ_{QPM} = 9.4 μm and Λ_{PM} = 1.92 mm when the crystal temperature is set to 70 °C.

3. DEVICE CHARACTERIZATION USING CLASSICAL LIGHT

We first characterized the phase-modulated QPM gratings using second-harmonic generation (SHG), sum- and difference-frequency generation (SFG and DFG). In the design of the crystal using the theoretical refractive indices[21], the crystal temperature where the wavelengths of the $|\mathrm{H_{sig}V_{idl}}\rangle$ and $|\mathrm{V_{sig}H_{idl}}\rangle$ are matched was 70 °C. However, initial measurements of the actual crystal showed that the real temperature was higher. Instead of operating near 70 °C, the PPLN device needed to be operated at 140 °C or higher in order to phasematch the pump wavelength near 775 nm, and signal and idler near 1550 nm. Figure 1a shows the measured SHG tuning curve for a phase-modulated QPM grating at 140 °C. Two peaks are clearly visible, indicating that two nonlinear processes are simultaneously phasematched.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 03/21/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

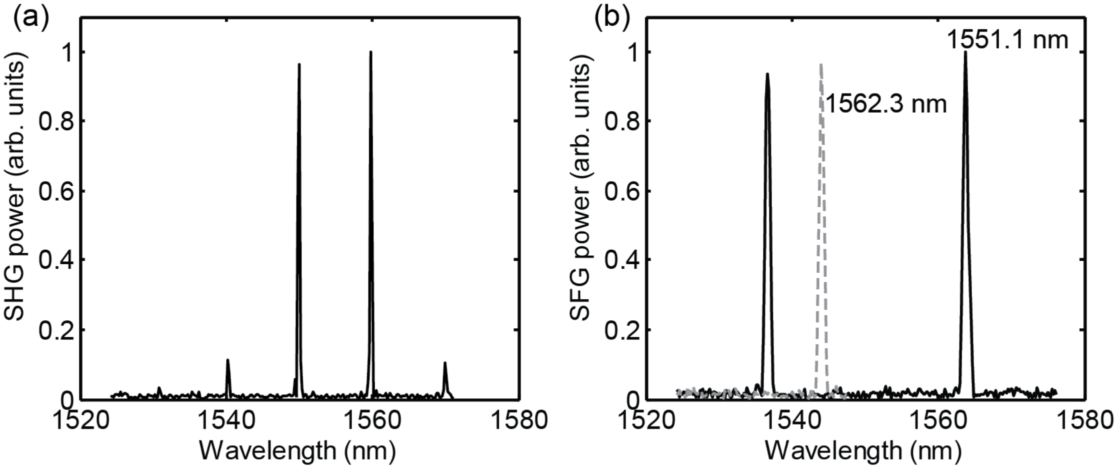


Figure 1. Measured (a) second-harmonic generation and (b) sum-frequency generation tuning curves at T=140 °C. For SHG, the fundamental beam is polarized at 45° to the crystal axes for the type-II interaction. For SFG, the vertically polarized beam is fixed to 1551.1 nm (solid) or 1562.3 nm (dashed) while the horizontally polarized beam is swept in wavelength. For the solid curve, both peaks are visible, while for the dashed curve, the second peak fell outside the tuning range of the laser around 1517 nm. The powers are given in arbitrary units (arb. units) with the maximum powers scaled to 1.

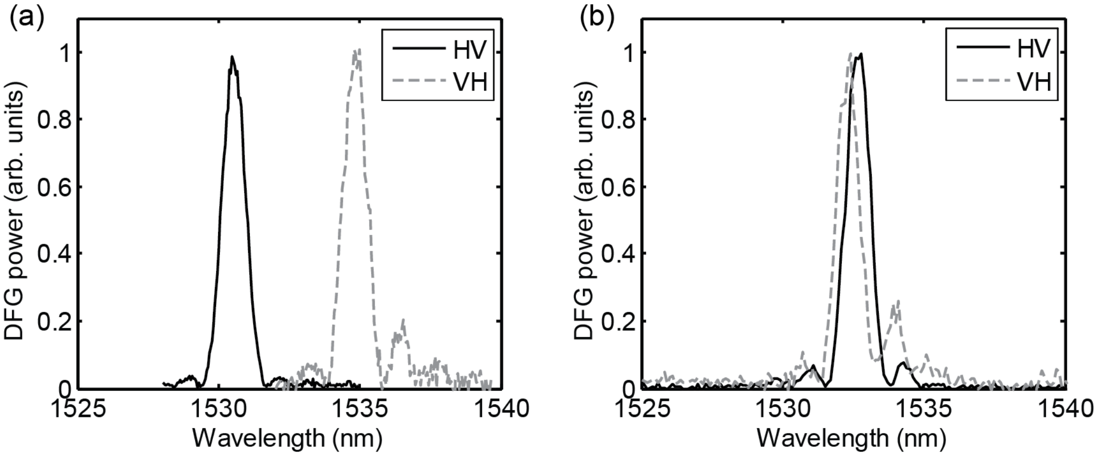


Figure 2. Difference-frequency generation spectra at two crystal temperatures, (a) 140 °C and (b) 143.5 °C. The horizontally polarized pump is fixed to 774.8 nm. The HV curve represents the state $|H_{sig}V_{idl}\rangle$; that is, the signal beam near 1530 nm is horizontally polarized while the corresponding idler near 1570 nm is vertically polarized. The maximum power is scaled to 1 for each trace.

We also observed SFG in the phase-modulated PPLN gratings. We used two continuous-wave, tunable, C-band, external cavity diode lasers. The two lasers were combined using a fiber beam combiner to ensure perfect co-alignment, and the beams were focused into the PPLN grating. Figure 1b shows observed sum-frequency tuning curves for the same grating at 140 °C. Since the nonlinear interaction is type-II, the two beams near 1550 nm must be orthogonally polarized. We fixed the vertically polarized beam to 1551.1 nm or 1562.3 nm wavelength and swept the horizontally polarized beam. The two traces in Fig. 1b are labeled by the wavelength of the fixed laser. Increasing the wavelength of the vertically polarized beam causes the tuning curve for the horizontal polarization to shift to shorter wavelengths.

After determining the proper operating temperature through the SHG and SFG measurements, we performed DFG using the phase-modulated QPM gratings. We used a fixed-wavelength, distributed feedback diode laser at 774.8 nm and a tunable external cavity diode laser near 1550 nm. A Glan-Thompson polarizer after the PPLN was used to reject the signal beam and transmit the generated difference-frequency (DF) beam. A 1550 nm dichroic edge filter was also used to improve separation of the signal and DF beams. The DF beam was detected with an InGaAs detector. Results of DFG measurements are presented in Fig. 2. At 140 °C, the spectrum for the $|H_{sig}V_{idl}\rangle$ process does not overlap with the

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 03/21/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

spectrum for the $|V_{sig}H_{idl}\rangle$ process. By increasing the temperature to 143.5 °C, we achieve good spectral overlap where $\lambda(H_{sig}) = \lambda(V_{sig}) = 1532.5$ nm. We also observed that the spectral bandwidths are nearly equal, which is important for preserving entanglement and not using additional filters.

It has been recently argued that such characterization with classical light is a fast and effective technique to infer information about the associated spontaneous emission processes that are later used for quantum entanglement[14]. Indeed, our seeded emission measurements inform us of the proper operating temperature and show that the spectra of the two processes are similar in bandwidth and in side-lobe structure. However, single-photon characterizations are still very important as ultimately, single-photon measurements are needed to observe quantum behavior.

4. OBSERVATION OF SPONTANEOUS EMISSION SPECTRA

4.1 Fiber-assisted, single-photon spectroscopy

Superconducting nanowire single photon detectors (SNSPDs) have remarkably high detection efficiency (up to 93% efficiency) and very small timing jitter (~100 ps)[22]. This fine temporal resolution can be translated to spectral resolution by incorporating a dispersive medium so that different wavelength components of the test light arrive at the detector at different times. This is the underlying principle of fiber-assisted, single-photon spectroscopy[15-17], where the dispersion is provided by a long length of optical fiber or a more compact fiber dispersion compensation module (DCM).

We first characterized the dispersion produced by the DCM. Figure 3a shows the measured relative time delay of different spectral components passing through the DCM. The slope of this data with respect to wavelength gives the dispersion, which is shown in Fig. 3b. At 1550 nm wavelength, the DCM produces -1.0 ns/nm dispersion. The negative sign of the dispersion indicates that longer wavelengths lead the shorter wavelengths.

Figure 4 shows the experimental setup. The domain-engineered PPLN crystal is pumped with a continuous-wave 775-nm wavelength laser that has a linewidth below 200 kHz. After the PPLN, the pump is filtered out with a dichroic mirror and the orthogonally polarized signal and idler photons are sent to a half-wave plate (HWP) and polarization beam splitter (PBS). For most measurements, the HWP is removed altogether or positioned to have no effect so that the horizontally polarized photons are transmitted and the vertically polarized photons are reflected by the PBS. For certain measurements, the HWP is positioned to produce 45° of polarization rotation, which effectively makes the PBS a non-polarizing beam splitter. After the beam splitter, both beams are coupled into optical fibers. We did not fully optimize the collection efficiency, which was around 5% to 10%. Since the fiber-assisted spectroscopy measurement requires clicks from both arms, mismatched collection efficiencies do not distort the spectral measurement but they do change the overall coincidence count rate. We incorporated DCMs into one or both of the arms after the beam splitter. With a single DCM, the undispersed arm after the PBS serves as a trigger while the other arm is dispersed by roughly 1 ns/nm. When two DCMs are used, the signal-idler dispersion is doubled at the expense of coincident count rate reduction since each DCM has about 4 dB loss. The photons were detected by SNSPDs and the arrival times analyzed with time-tagging electronics.

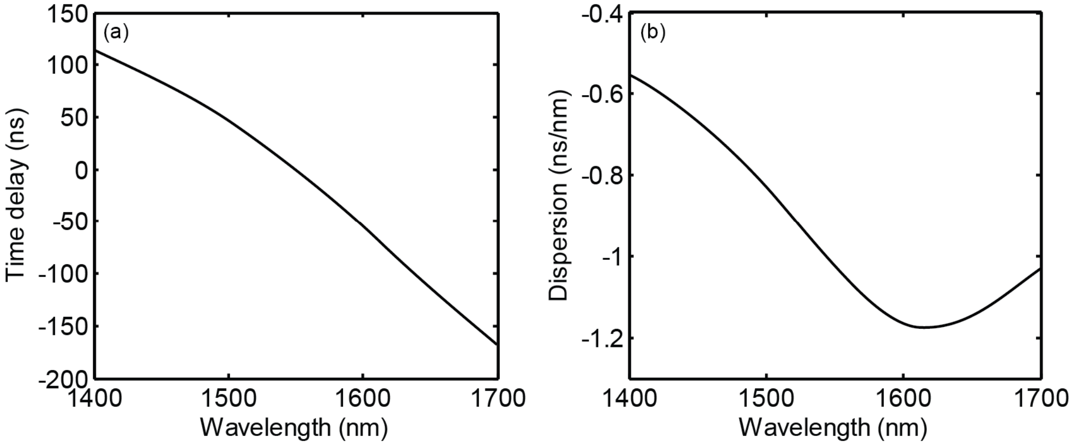


Figure 3. (a) Relative time delay of different wavelengths passing through the dispersion compensation module. (b) Dispersion produced by the DCM. At 1550 nm, the dispersion is -1 ns/nm.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 03/21/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

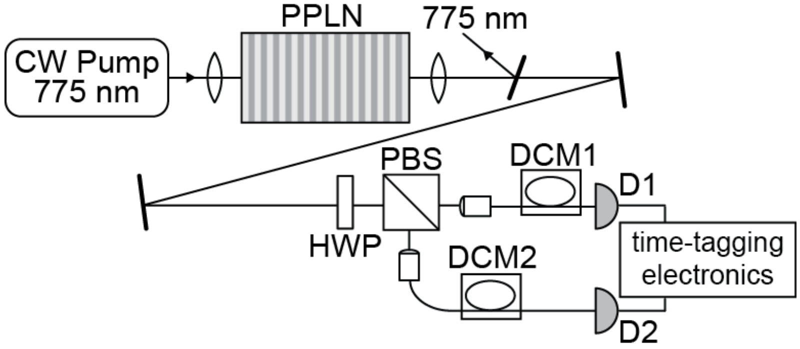


Figure 4. Sketch of experimental setup. The PPLN crystal is pumped by a CW 775 nm laser. Horizontally and vertically polarized photons near 1550 nm are produced by SPDC. The down-converted photons are incident on a beam splitter (polarizing beam splitter when the HWP is removed, and non-polarized beam splitter when the half-wave plate (HWP) rotates polarizations by 45°) and then coupled into optical fibers. The light is dispersed with dispersion compensation modules DCM1 and/or DCM2 then detected by SNSPDs. Arrival times are logged using time-tagging electronics.

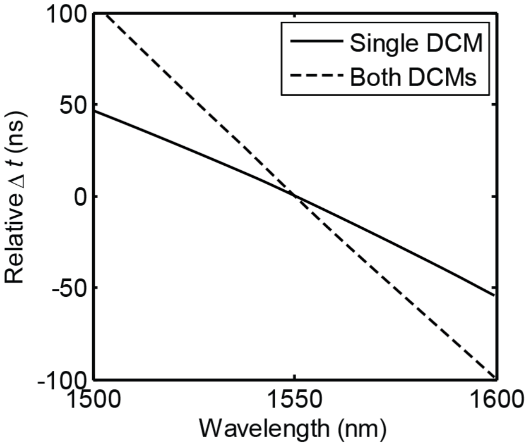


Figure 5. Map between wavelength and relative difference in arrival times of photons at D1 and D2 (Δt) for single DCM in only one arm of the experiment, and DCMs in both arms of the experiment (as sketched in Fig. 4). A larger spread in arrival times is obtained with both DCMs than with a single DCM. We set $\Delta t = 0$ for 1550 nm, which is $2\lambda_{\text{pump},}$ where the signal and idler wavelengths would be degenerate.

Using the dispersion data in Fig. 3 and the fact that the pump is narrowband, we can map the difference in arrival times of photons at D1 and D2 (in Fig. 4) to the signal-idler pair that produced the pair of clicks. This mapping is shown in Fig. 5. In Fig. 5, we see that when using two DCMs produces roughly twice more temporal spread for the same signal-idler wavelengths as one DCM. The *y*-axis of this figure is given in relative delay, with Δt set to 0 at 1550 nm wavelength. We also note that each DCM produces 30 μs of fixed delay. We calibrate the delay caused by experimental path imbalances by examining data where the HWP and PBS together act as a non-polarizing beam splitter and look for symmetry when the measured data are reflected about $2\lambda_{\text{pump}}$.

4.2 Measured single-photon spectra

Spectra taken using a single DCM are shown in Fig. 6. The PPLN temperature was 138 °C. We used 1 minute integration time for this data with 3 mW CW pump power incident on the PPLN crystal. The *x*-axis represents the wavelength of the H-polarized photons. In Fig. 6a, we show the effect of inserting the HWP before the PBS. Without the HWP, the H-polarized photons are sent to D1 and the V-polarized photons are sent to D2 (with DCM2 in the V-arm to disperse the wavelengths and no DCM in the H-arm). Two peaks are visible, which correspond to the two SPDC processes $|H_{\text{sig}}V_{\text{idl}}\rangle$ and $|V_{\text{sig}}H_{\text{idl}}\rangle$. When the HWP is inserted before the PBS, all four possible signal and idler photons are sent to both arms. The measurement records coincidences in D1 and D2, which reflect the pairs of photons generated by SPDC. Since now the H-polarized and the V-polarized photons pass through DCM2, we see twice the number of

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 03/21/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

peaks. Specifically, the peak at 1529 nm is the same process that corresponds to the peak at 1571 nm (and similarly for the peaks at 1536 nm and 1564 nm). In Fig. 6b, we compare spectra measured with only DCM1 in the H-arm or only DCM2 in the V-arm. We see that the spectrometer works well in either configuration; the spectra show excellent agreement especially in the fine structure of the side lobes.

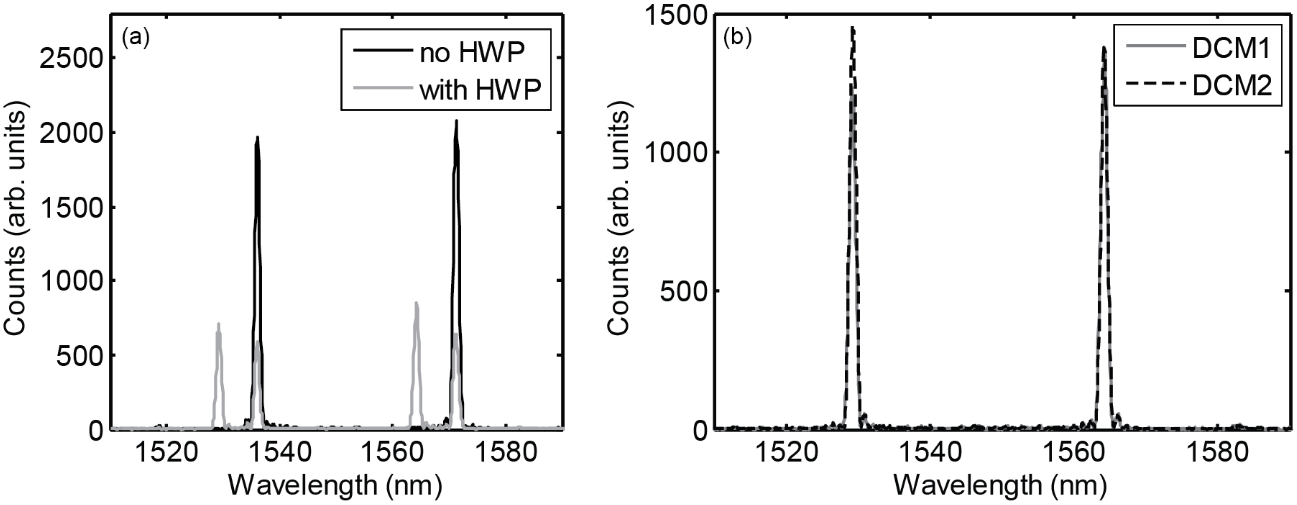


Figure 6. (a) SPDC spectra measured using only DCM2 with and without the half-wave plate. The HWP sends all four photons to both arms, which leads to the apparent splitting of the peaks. (b) SPDC spectra measured without the HWP and with a single DCM in the experiment in the H-arm (DCM1) or the V-arm (DCM2). There is excellent agreement in the observed spectra.

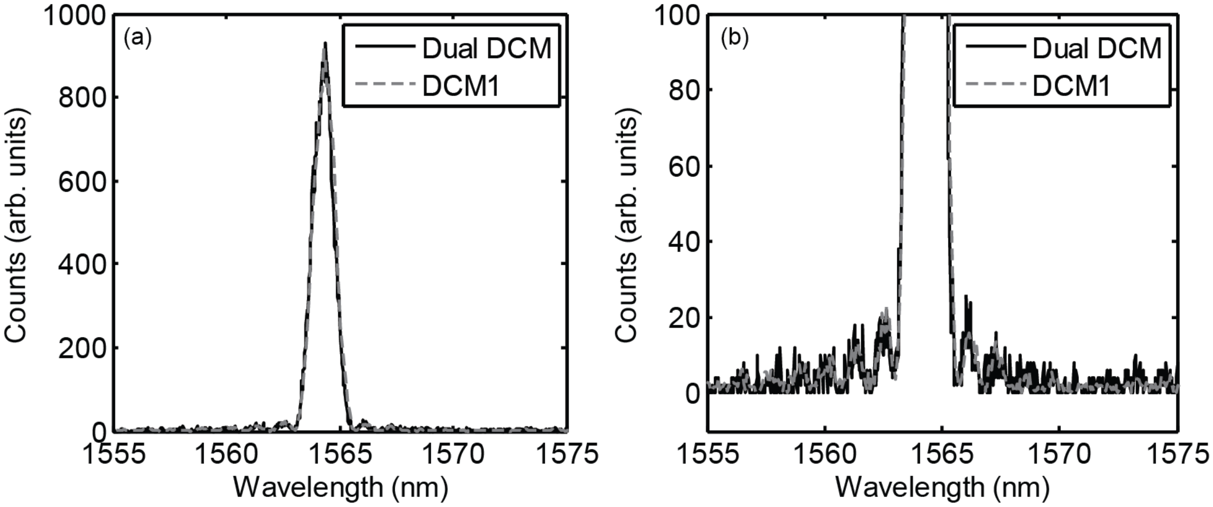


Figure 7. Comparison of spectra measured with DCMs in both arms after the PBS and with DCM1 in the H-arm only. The PPLN temperature is set to 138 °C. (b) is a zoom in of (a). Peaks are scaled to equal heights and counts are shown in arbitrary units. There is agreement in the spectra, but the data using dual DCMs show worse signal-to-noise ratio.

We also measured SPDC spectra using DCMs in both arms of the experimental setup. Having two DCMs compared to a single DCM in the setup caused the coincidence rate to drop by a factor of 10. To compensate for the lower count rates, we integrated for 3 minutes instead of the 1 minute used for single DCM measurements. Figure 7 shows a comparison of the spectra measured with dual and single DCM. In these measurements, the PPLN temperature was at 138 °C. We focus on the peak near 1564 nm. We scaled the data to have equal maxima and zoom in to examine the side lobes in Fig. 7b. There is good agreement in the two traces. Even though the dual DCM measurement had three times longer integration time, because of the low coincidence count rate, the signal-to-noise rate was worse than the DCM1 measurement.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 03/21/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

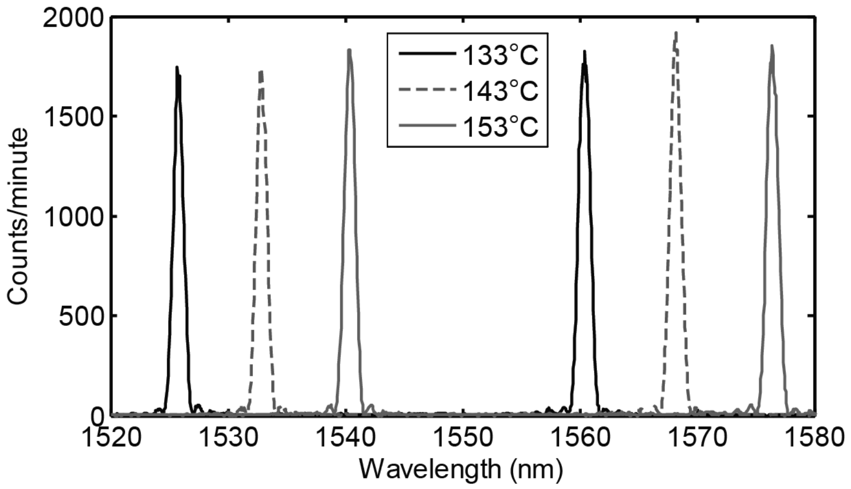


Figure 8. Temperature tuning of the domain-engineered PPLN crystal. Each trace is measured with no HWP, DCM1 in the setup, and an integration time of one minute.

Figure 8 illustrates temperature tuning of SPDC produced by the domain-engineered PPLN crystal. The spectra were measured with a single DCM in the setup (DCM1), no HWP and one minute integration time. At PPLN temperature of 143°C, we achieve $\lambda(H_{sig}) = \lambda(V_{sig})$ and $\lambda(V_{idl}) = \lambda(H_{idl})$ and the two processes $|H_{sig}V_{idl}\rangle$ and $|V_{sig}H_{idl}\rangle$ become indistinguishable in wavelength. At this temperature, the two peaks become equally spaced about $2\lambda_{pump}$ = 1550 nm. In contrast, the spectrum measured with the HWP in Fig. 6a clearly show that at 138 °C, $\lambda(H_{sig}) \neq \lambda(V_{sig})$ and $\lambda(V_{idl}) \neq \lambda(H_{idl})$. The single-photon spectra shown in Figs. 6 through 8 are in good agreement with seeded spectra (Fig. 2).

5. DISCUSSION

We characterized the down-conversion spectra of the domain-engineering PPLN crystal at both the classical and single-photon light levels. There was good agreement between the single-photon and seeded measurement results. Also, the spectra agree well with theoretical predictions based on the QPM domain design. The 35 nm spacing between the two peaks was as designed, and the observed peaks had sinc^2-like shapes. The only design discrepancy was the operating temperature, which was about 70 °C higher than theoretically predicted. The phase-modulated QPM structure also produced small satellite peaks around 1500 nm and 1600 nm in wavelength, just outside the range of the spectrum plotted in Fig. 6b. These satellite peaks were both predicted theoretically and observed experimentally.

This technique to measure single-photon SPDC spectra, fiber-assisted single-photon spectroscopy, is a very powerful and fast way to characterize SPDC sources. We show here that it works well for CW-pumped SPDC while pulsed pumping was shown previously[15-17]. We easily acquired spectra spanning ~100 nm with 1 minute integration, which is arguably faster than using a single-photon detector and scanning the spectrum with a monochromator. In fact, our difference-frequency generation measurements (performed by scanning the laser wavelength and recording the InGaAs photodiode response) took about 5 minutes to acquire, yet the DFG spectra (Fig. 2) seem noisier than the single-photon spectra with 1 minute acquisition time shown in Fig. 8. The advantages of the fiber-assisted single-photon spectral measurements can be attributed to the high performance of the SNSPDs and the fast data collection using the time-tagging electronics. The DFG spectra were taken using a chopper, lock-in amplifier and battery-powered InGaAs biased photodiode. This classical light measurement has a much higher noise floor than measurements using SNSPDs.

In our future work, we plan to measure the entanglement visibility of our source. Good entanglement requires the two processes be indistinguishable. The observed spectra show the point where the wavelengths of the two processes are matched (T=143 °C). The amplitudes and widths of the two peaks are also nearly the same. We must implement temporal compensation to erase the effects of the PPLN birefringence, which causes the different polarizations to walk-off in time and become distinguishable by their relative arrival times[23]. Our measurements here indicate that the domain-engineering PPLN SPDC source has the potential to produce high-quality quantum entanglement.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 03/21/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

6. CONCLUSION

We have designed and characterized an engineered nonlinear crystal for use as a source of polarization-entangled photon pairs. The PPLN crystal uses a phase-modulated QPM grating design to phasematch the generation of $|H_{sig}V_{idl}\rangle$ and $|V_{sig}H_{idl}\rangle$ states in a single crystal. We performed stimulated and spontaneous emission down-conversion spectral measurements on the crystal and observed the two simultaneous processes, which operate at 775 nm → 1532.5 nm + 1567.5 nm when the wavelengths are matched. We demonstrate that CW-pumped SPDC can be effectively characterized by fiber-assisted single-photon spectroscopy. These results are promising signs that our crystal can perform well in quantum entanglement applications.

REFERENCES

[1] Kwiat, P. G., Mattle, K., Weinfurter, H., Zeilinger, A., Sergienko, A. V., and Shih, Y., "New high-intensity source of polarization-entangled photon pairs," Phys. Rev. Lett. 75(24), 4337-4341 (1995).

[2] Kurtsiefer, C., Oberparleiter, M., and Weinfurter, H., "High-efficiency entangled photon pair collection in type-II parametric fluorescence," Phys. Rev. A 64, 023802 (2001).

[3] Fejer, M. M., Magel, G. A., Jundt, D. H., and Byer, R. L., "Quasi-phase-matched second harmonic generation: tuning and tolerances," IEEE J. Quantum Electron. 28(11), 2631-2654 (1992).

[4] Tanzilli, S., De Riedmatten, H., Tittel, W., Zbinden, H., Baldi, P., De Micheli, M., Ostrowsky, D. B., and Gisin, N., "Highly efficient photon-pair source using periodically poled lithium niobate waveguide," Electron. Lett. 37(1), 26-28 (2001).

[5] Da Cunha Pereira M., Becerra, F. E., Glebov, B. L., Fan, J., Nam, S., and Migdall, A., "Demonstrating highly symmetric single-mode, single-photon heralding efficiency in spontaneous parametric downconversion," Opt. Lett. 38(10), 1609-1611 (2013).

[6] Tanzilli, S., Tittel, W., Halder, M., Alibart, O., Baldi, P., Gisin, N., and Zbinden, H., "A photonic quantum information interface," Nature 437, 116-120 (2005).

[7] Suhara, T., Nakaya, G., Kawashima, J, and Fujimura, M., "Quasi-phase-matched waveguide devices for generation of postselection-free polarization-entangled twin photons," IEEE Photon. Technol. Lett. 21(15), 1096-1098 (2009).

[8] Ueno, W., Kaneda, F., Suzuki, H., Nagano, S., Syouji, A., Shimizu, R., Suizu, K., and Edamatsu, K., "Entangled photon generation in two-period quasi-phase-matched parametric down-conversion," Opt. Express 20(5), 5508-5517 (2012).

[9] Herrmann, H., Yang, X., Thomas, A., Poppe, A., Sohler, W., and Silberhorn, C., "Post-selection free, integrated optical source of non-degenerate, polarization entangled photon pairs," Opt. Express 21(23), 27981-27991 (2013).

[10] Kuo, P. S., Pelc, J. S., Slattery, O., Kim, Y.-S., and Tang, X., "Entangled photon generation in a phase-modulated, quasi-phasematched crystal," Proc. SPIE 8875, 887508 (2013).

[11] Kuo, P. S., Pelc, J. S., Slattery, O., Ma, L., and Tang, X., "Domain-engineered PPLN for entangled photon generation and other quantum information applications," Proc. SPIE 9136, 913603 (2014).

[12] Trojek, P., and Weinfurter, H., "Collinear source of polarization-entangled photon pairs at nondegenerate wavelengths," Appl. Phys. Lett. 92, 211103 (2008).

[13] Steinlechner, F., Trojek, P., Jofre, M., Weier, H., Perez, D., Jennewein, T., Ursin, R., Rarity, J., Mitchell, M. W., Torres, J. P., Weinfurter, H., and Pruneri, V., "A high-brightness source of polarization-entangled photons optimized for applications in free space," Opt. Express 20(9), 9640-9649 (2012).

[14] Liscidini, M., and Sipe, J. E., "Stimulated Emission Tomography," Phys. Rev. Lett. 111, 193602 (2013).

[15] Avenhaus, M., Eckstein, A., Mosley, P. J., and Silberhorn, C., "Fiber-assisted single-photon spectrograph," Opt. Lett. 34(18), 2873-2875 (2009).

[16] Gerrits, T., Stevens, M. J., Baek, B., Calkins, B., Lita, A., Glancy, S., Knill, E., Nam, S. W., Mirin, R. P., Hadfield, R. H., Bennink, R. S., Grice, W. P., Dorenbos, S., Zijlstra, T., Klapwijk, T., and Zwiller, V., "Generation of degenerate, factorizable, pulsed squeezed light at telecom wavelengths," Opt. Express 19(24), 24434 (2011).

[17] Gerrits, T., Marsili, F., Verma, V. B., Shalm, L. K., Shaw, M., Mirin, R. P., and Nam, S. W., "Spectral correlation measurements at the Hong-Ou-Mandel interference dip," Phys. Rev. A 91, 013830 (2015).

[18] Asobe, M., Tadanaga, O., Miyazawa, H., Nishida, Y. and Suzuki, H., "Multiple quasi-phase-matched $LiNbO_3$ wavelength converter with a continuously phase-modulated domain structure," Opt. Lett. 28(7), 558-560 (2003).

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 03/21/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

[19] Asobe, M., Tadanaga, O., Miyazawa, H., Nishida, Y., and Suzuki, H., "Multiple quasi-phase-matched device using continuous phase modulation of $\chi^{(2)}$ grating and its application to variable wavelength conversion," IEEE. J. Quantum Electron. 41(12), 1540-1547 (2005).

[20] Pelc, J. S., Kuo, P. S., Slattery, O., Ma, L., Tang, X., and Fejer, M. M., "Dual-channel, single-photon upconversion detector at 1.3 μm," Opt. Express 20(17), 19075-19087 (2012).

[21] Gayer, O., Sacks, Z., Galun, E., and Arie, A., "Temperature and wavelength dependent refractive index equations for MgO-doped congruent and stoichiometric $LiNbO_3$," Appl. Phys. B 91, 343-348 (2008).

[22] Marsili, F., Verma, V. B., Stern, J. A., Harrington, S., Lita, A. E., Gerrits, T., Vayshenker, I., Baek, B., Shaw, M. D., Mirin, R. P., and Nam, S. W., "Detecting single infrared photons with 93% system efficiency," Nat. Photon. 7, 210-214 (2013).

[23] Shih, Y., "Entangled photons," IEEE J. Sel. Topics Quantum Electron. 9(6), 1455-1467 (2003).

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 03/21/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

A virtual milling machine model to generate machine-monitoring data for predictive analytics

David Lechevalier[1/2], Seung-Jun Shin[1], Jungyub Woo, Sudarsan Rachuri[1], Sebti Foufou[3]

[1]National Institute of Standards and Technology, Gaithersburg, USA
david.lechevalier@nist.gov
seungjun.shin@nist.gov
jungyub.woo@nist.gov
sudarsan.rachuri@nist.gov

[2]Le2i, Université de Bourgogne, Dijon, France
david_lechevalier@etu.u-bourgogne.fr

[3]CSE Department, College of Engineering, Qatar University, Qatar
sfoufou@qu.edu.qa

Abstract. Real data from manufacturing processes are essential to create useful insights for decision-making. However, acquiring real manufacturing data can be expensive and time consuming. To address this issue, we implement a virtual milling machine model to generate machine monitoring data from process plans. MTConnect is used to report the monitoring data. This paper presents 1) the characteristics and specification of milling machine tools, 2) the architecture for implementing the virtual milling machine model, and 3) the integration with a simulation environment for extending to a virtual shop floor model. This paper also includes a case study to explain how to use the virtual milling machine model for predictive analytics modeling.

Keywords: STEP, MTConnect, milling, data generator, data analytics

1 Introduction

The application of data analytics in manufacturing is one of the most promising methods to help manufacturers improve the productivity of their systems by saving money and time or reducing process flaws. Collecting manufacturing data is critical to make use of the different techniques available for data analytics. In the framework described in [1], the authors described the importance and the necessity of data collection to run data analytics in the manufacturing area, which continuously generates large amounts of data [2]. Data can be in different formats that can be defined as structured or unstructured. The suggested framework needs to be able to understand these different data formats to analyze the data. In particular, modern machines are able to provide real-time data to monitor the values of operating parameters. This data can be specified in the MTConnect standard [3] in order to facilitate the communication between equipment and software applications.

Lechevalier, David; Shin, Seungjun; Woo, Jungyub; Rachuri, Sudarsan; Foufou, Sebti.
“A virtual milling machine model to generate machine-itoring data for predictive analytics.”
Paper presented at the The Product Lifecycle Management (PLM) Conference 2015, Doha, Qatar, Oct 19-Oct 21, 2015.

However, since acquiring data is still expensive and time consuming, simulation approaches that can generate data at a lower cost need to be explored. Simulation approaches have already allowed manufacturers to reduce costs and time at the factory level [4] by generating simulated data that they can analyze to improve the performance of their systems. While creating virtual machine models can allow manufacturers to generate simulated process data, using these models together will lead to a virtual shop floor model at the production level.

Combining simulation and data analytics at the process level can lead to a process efficiency improvement at a lower cost. In [5], authors have compared Bayesian Networks and Artificial Neural Networks for running analytics on real and simulated data with efficient results to predict the output values.

This paper introduces a virtual milling machine model to generate machine monitoring data from a process plan. In addition to the model, we also present an agent-based model including a machine-state-chart diagram. We integrate our virtual machine model into the agent model to use it in a simulation environment. We show how the agent-based model and the virtual machine model can be embedded in a shop-floor-level simulation environment combining discrete event and agent-based models. Finally, we illustrate how data analytics can be applied.

This paper is organized as follows: Section 2 introduces the characteristics and specifications of the virtual milling machine model. Section 3 presents the virtual milling-machine model, and its combination with an agent-based model into a simulation environment. Section 4 shows how a manufacturer can leverage this combination and use the generated data to run analytics for system improvement.

2 Specifications of the Virtual Milling Machine Model

In this section, we present the specification of input and output data for our virtual model. We also introduce the equations needed to compute the power metrics related to the milling process and finally show the state chart that we define for representing the behavior of a machine and include our model in a simulation environment.

2.1 Input data and output data: from STEP-NC program file to MTConnect document

We identify an ISO 14649 STEP-NC [6] program file (henceforth referred to as STEP-NC file) and MTConnect document respectively as input and output data of our virtual model. In [7], authors underline that a STEP-NC-based approach is promising for digital manufacturing while authors emphasize MTConnect capabilities to improve the interoperability of machine tools in [8]. Numerical control (NC) programs allow manufacturers to automatically control machine tools. The use of NC machines and computers in manufacturing led to the development of computer-aided manufacturing (CAM) where computers interpret CAM files to send a set of instructions to the NC machines in order to achieve the production defined in the original CAM file.

MTConnect is an XML-based [9] standard to represent machine monitoring data. This standard aims to provide interoperability so that manufacturers can monitor various brands and models of Computer Numerical Control (CNC) machines through a common interface. By using this standard for the output data, we ensure that the data will have a well-known structure that facilitates the communication for later uses.

2.2 Machine tool specification for kinematics and dynamics

To virtually model a milling machine, we compute kinematics (e.g., velocity and position) and dynamics (e.g., force and power) corresponding to the events and movements of the machine tool. A STEP-NC program specifies a sequence of machining operations, and is used to create an NC program in the ISO 6983 (G-Code) format [10]. Meanwhile, an MTConnect document generates continuous snap shots of a machine tool's actions and events using time as reference. Thus, for every instruction of the NC program, we need to compute the corresponding metrics of the machine tool. Computing these metrics requires equations that are derived from physical model-based analysis of machine tool metrics. We make a calculation of power, which indicates the amount of energy consumed per unit-time.

First, we defined a position function by deriving theoretical equations presented in [11]. This function is presented in Equation (1) assuming that linear velocity has a trapezoidal profile.

$$\begin{aligned}
&\mathit{if}\ 0 \le t \le t_a,\quad \mathit{then}\ L_i(t) = 0.5 a_L t^2 \\
&\mathit{else\,if}\ t_a \le t < t_a + t_s,\quad \mathit{then}\ L_i(t) = 0.5 a_L t_a^2 + v_i (t - t_a) \\
&\mathit{else\,if}\ t_a + t_s \le t < t_a + t_s + t_d,\quad \mathit{then}\ L_i(t) = 0.5 a_L t_a^2 + v_i t_s + 0.5T(2v_i - a_L T), T = t - t_a - t_s
\end{aligned} \quad , (1)$$

where L: length from a previous point (mm), t: the current time (ms), t_a: acceleration time (ms), t_s: steady-state time (ms), t_d: deceleration time (ms), v_i: velocity on each axis (m/s).

Using this function, our virtual machine model computes the kinematics that include linear-axial positions as a function of time. These position data can be used to detect cutting or non-cutting motions that occur between a work piece and a cutting tool. The characterization of the motions contributes to determine the power consumption.

Second, our virtual model computes the machine tool dynamics using theoretical equations introduced in [12]. The power profile of a single NC code command for linear movement consists of acceleration, steady and deceleration states. Power during the steady state varies for cutting and non-cutting motions. During the cutting motion, the power corresponds to the cutting power, which is caused from cutting forces, plus the idle power. We use a physics-based equation, as expressed in Equation (2), to calculate the cutting forces. Equations (3) and (4), respectively, present the linear-axial and rotary-axial power for a milling machine. Units can be obtained in the reference paper [12].

$F_t = K_{tc}bh + K_{te}b$ $F_f = K_{fc}bh + K_{fe}b$ (2)	$P_{L,a} = \frac{T_a w}{\eta_L}, \quad T_a = J_e \frac{dw}{dt} + Bw + T_s$ $P_{L,s} = \frac{T_s w}{\eta_L}, \quad T_s = (T_{gf} + \frac{\mu_b d_p (F_f + F_p)}{2} + T_f) / r_g$ $P_{L,d} = \frac{T_d w}{\eta_L}, \quad T_d = -J_e \frac{dw}{dt} + Bw - T_s$ (3)	$P_{S,a} = \frac{(T_{S,a} + T_{run})w}{\eta_S}$ $P_{S,s} = \frac{T_{run} w}{\eta_S}$ $P_{S,c} = P_{S,s} + \frac{2\pi F_c v_c}{\eta_S}$ $P_{S,d} = \frac{(-T_{S,a} + T_{run})w}{\eta_S}$ (4)

2.4 Machine states

To integrate our virtual milling machine model inside an agent-based model, we develop a state chart that represents the different states of the machine. The model is presented below in **Figure 1**.

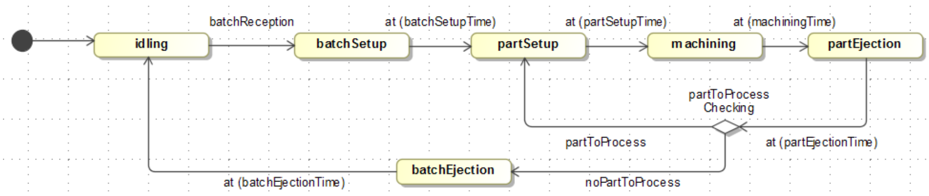


Figure 1. State chart diagram for a machine

The default machine state is the *idling* state. As soon as a batch arrives (represented by the transition *batchReception* in the figure), the machine goes to the next state called *batchSetup*. This state models the required machine setup for processing the batch. Once the batch is setup, the machine goes to the *partSetup* state where the machine sets up each part to execute the needed operations. The next state called *machining* represents the milling process. Once the operations have been executed on the part, the machine goes to the *partEjection* state that models unloading of the part. After this state, two alternative paths can be taken by the machine in the state chart. If there are still parts to process in the batch, the machine goes back to *partSetup*. In the other case, the machine goes to the last state, which is the *batchEjection* state, when the batch unload step is modeled. After a batch has been ejected, the machine goes back to the *idling* state waiting for a new batch.

3 Description of the virtual machine model architecture and integration in an agent-based model

In the previous section, we have shown the specifications that define our virtual machine model. In this section, we introduce the architecture of the virtual machine model that makes it possible to generate machine monitoring data virtually. We then present the integration of the virtual model inside an agent-based model. We finally discuss the benefits of this integration.

3.1 Architecture of the virtual machine model

Figure 2 illustrates the process flow (including involved tools and generated outputs for each step) followed by the virtual milling machine model to generate MTConnect data. The virtual milling machine model takes, as an input, a STEP-NC file. The model parses and interprets this file using a toolkit for Parts 10, 11, and 111 (related to milling process data and tools) that is written in C++ and referred to as ISO 14649 Toolkit in the picture. This toolkit has been developed at the National Institute of Standards and Technology (NIST) for programing with ISO 14649, Parts 10 and 11, and is being applied to study different ISO 10303 [13] application-protocol file characteristics and their interpretation [14]. Using this toolkit, we can generate the sequence of G-Code instructions. We developed a physics-based modeler that we have integrated in our virtual model to transform the G-Code instructions into machine tool kinematics and dynamics.

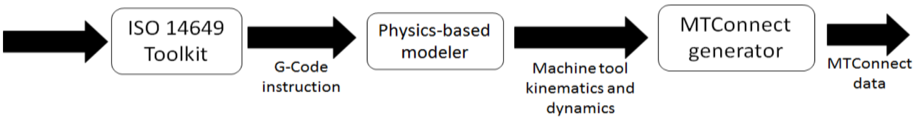


Figure 2. Step-by-step procedure of the virtual milling machine model

The computed movement metrics are length, acceleration, velocity, time, cutting, force and power. Computations are based on the equations introduced in the previous section. You can see below, in **Figure 3**, a class diagram representing the movement structure. For brevity, we show an overview of the class diagram. We define an abstract class called *Movement*. This class is extended by another abstract class called *StraightMovement* that is itself an extension by two classes called *TraverseStraightMovement* and *FeedStraightMovement*. These two last classes allow representation as two different movement types for the milling machine. The schema can be extended to represent additional movement types in the future. All the computed metrics are also represented as classes and are aggregated to the Movement class. The class Power is abstract and is extended by two classes: TraversePower and FeedPower that will represent the power depending on the movement type. The physics-based modeler instantiates this structure during the computations and generates a Movement collection that represents the machine tool kinematics and dynamics.

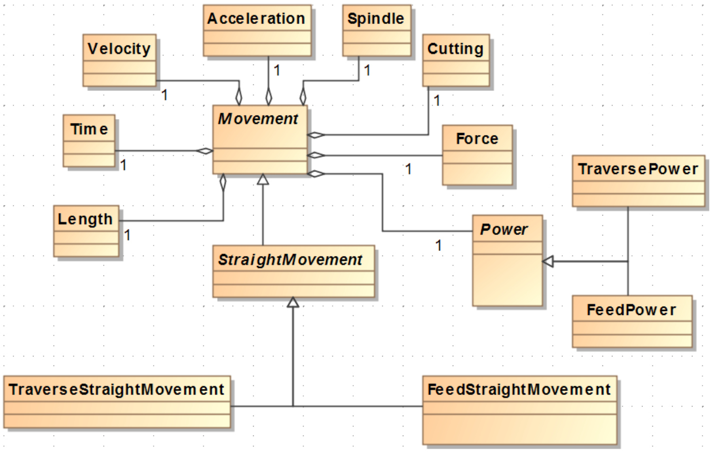


Figure 3. Class diagram representing the structure of a movement

To generate an MTConnect file corresponding to this STEP-NC file, we generate time series data representing the current position of the machine tool and the consumed power of the milling machine. Using the kinematics and dynamics that we generated in the previous step and an MTConnect generator that we developed as part of the virtual machine model, we generate MTConnect data representing the tool position and the consumed power every 100 milliseconds. We store these data in an MTConnect agent, which is a web service that collects the generated MTConnect samples. This MTConnect agent provides query functions that can be called to get specific sets of data previously stored.

3.2 Combination of the virtual machine model into an agent-based model using a simulated environment

To run our virtual machine model in a simulation environment, we integrate this virtual machine model in an agent–based model. The software environment called AnyLogic [15] allows us to extend the states and the transitions of a state chart using Java code. While implementing the state chart in an agent-based model, we can call virtual machine model functions by importing a Java ARchive (JAR) file that contains the needed functions. We first implement the state chart introduced in section **2.4** in the agent-based model. We extend this state chart by implementing additional Java code to initialize the parameters needed for the virtual machine model functions. During the batchSetup state, we get the time needed by the machine to set up the batch as well as the power consumed during this step by reading the machine specification described using XML. By following the same steps during the *partSetup* state, we generate the values of the machine parameters that depends on the properties of the material used for this batch. During the *machining* state, we include the parameters values inside a STEP-NC file given as an input to the virtual machine model. Using the appropriate functions, we can compute the machining time and the consumed power corresponding to the STEP-NC file given as input. In *partEjection* state and *batchEjection* state, we collect time and power consumed to achieve these ejection operations by reading the machine specification as we do for the setup states. All the values of time and power are subjects to a standard deviation to represent the uncertainty at a real machine level. Once a batch has been processed (after the *batchEjection* state), we generate Comma Separated Values (CSV) and MTConnect output files that gives the time and the power consumed by the milling machine.

3.3 Benefits

This approach provides benefits for manufacturing simulation. The simulation applications reviewed in [16] illustrate the interest in simulation in the manufacturing area. While simulations for manufacturing operations, such as planning or scheduling or real-time control, seem to be the most important trend, generating machine-monitoring data can lead to a more accurate simulation. The agent-based model implementation allows manufacturers to use the milling model in a very easy way since the agent-based model can be used directly to represent one machine. Thus, the virtual milling model generates data during the simulation representing real machine behavior. Moreover, agent updates are regularly possible. Collecting real data punctually makes it possible to calibrate the virtual model. It also enables including realistic noise in the simulated data to give more accuracy to the virtual model. Finally, the agent-based model can be improved by integrating disturbances such as machine failure in the state chart.

Extending this approach, providing a library of agents can allow manufacturers to choose the machine model to represent the machine involved in their manufacturing systems. Updates on virtual machine models only require a library update. A manufacturer can use an agent from the library in the simulation without really knowing how the integrated virtual model is implemented. Finally, different agents representing the same machine can provide different capabilities depending on the studied problem such as power consumption, flow capabilities and material consumption by integrating a different virtual model.

4 Use Case

In this section, we will illustrate how to use the agent-based model to generate data. We will first present the specification of our use case, and then show the implementation in the simulation environment. The last part introduces the application of regression analysis to generate an analytical model.

4.1 Use case scenario

We define a scenario to represent a milling machine in the simulated environment. In this scenario, a milling machine tool manufactures a steel part, as shown in **Figure 4**. The process parameters – feed rate, spindle speed, and cutting depth – control the tool path strategies that are necessary to make the given machining features. We assign the three process parameters randomly using a uniform distribution within the ranges given in **Table 1**. This process plan decision generates STEP-NC files. Each STEP-NC file is assigned to produce one part.

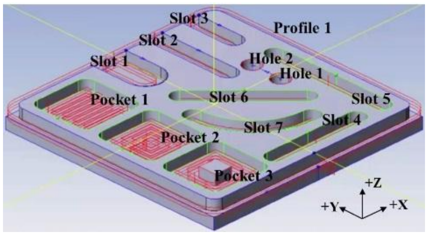


Figure 4. An example of a milling part

Table 1. Process plan data

Process parameter	Unit	Lower bound	Upper bound
Feedrate	mm/s	30	90
Spindle speed	rad/s	75.4	226.2
Cutting depth	mm	2.5	3.5

4.2 Implementation results

Given the process plan scenario in Section 4.1, we instantiate the agent-based model in a process flow model to collect MTConnect data. This process flow represents a flow of batch coming to the milling machine. Our machining model generates MTConnect documents for every part of the batch. To reproduce a real machine behavior, using an identical set of process parameters leads to different power values representing the variation that can occur in a real machine (±10 % uniform-random deviation during feed movement, and ±5 % uniform-random deviation during traverse movement). Using the agent-based model, we generate MTConnect time series data after every part ejection while running the simulation.

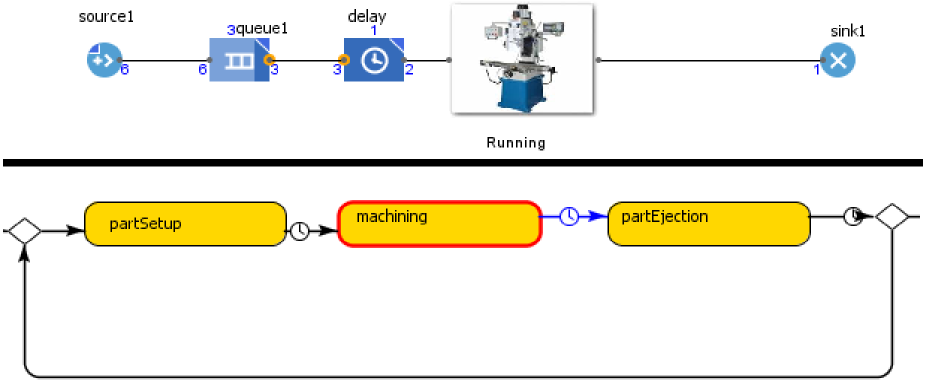


Figure 5. Example of simulation at the process flow and the agent levels.

Figure 5 shows the implementation of the scenario in Anylogic at the process and agent levels. The MTConnect document provides the following set of information: *x_axis_position*, *x_axis_wattage*, *y_axis_position*, *y_axis_wattage*, *z_axis_position*, *z_axis_wattage, c_axis_wattage*, *electric_wattage* and *coolant_wattage*.

4.3 Predictive modeling using generated data

Using the simulated data, we are able to run regression analysis to generate an analytical model by using machine learning techniques. This analytical model can then be used to predict values of the power consumption. After a normalization of the data, we train a neural network model with the first 500 samples of our simulated data. We give 300 new samples as inputs of the trained model and compare the outputs of the model and the simulated data generated by our virtual machine model using the same input parameters. **Figure 6** represents the comparison between the simulated total power (X-axis) and the predicted total power (Y-axis).

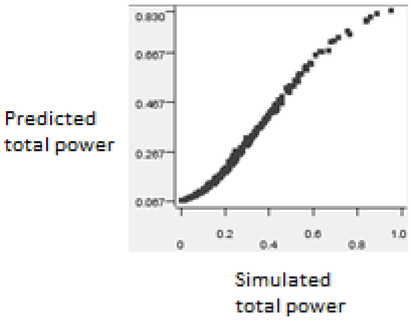


Figure 6. Scatter plot of the simulated and the predicted total power.

As you can see, the plot shows a slightly curved line showing that the predicted data are really close to the simulated data for the same input parameters. The coefficient of determination, representing how close the predicted data are to the simulated data, is 0.986. By applying this approach and after validation, a manufacturer can also use this model to compare the real outputs with the model outputs to establish diagnostic on a machine in a manufacturing system. Extending it to a full manufacturing system will allow a manufacturer to anticipate the behavior of the system in a simulation environment by taking advantage of the simulated data.

5 Conclusion

In this paper, we introduce a virtual milling machine model that allows us to generate machine-monitoring data in MTConnect format. We show that we can integrate this model in a simulated environment to take advantage of the generated data and generate a predictive model to finally improve or make a diagnostic on a milling process described in a STEP-NC file. In a future work, integration of maintenance and failure in our model can make our generation of data more realistic and improve our simulation. Moreover, taking advantage of our model and other existing models [17], we will be able to develop a virtual shop floor model.

DISCLAIMER
No approval or endorsement of any commercial product by NIST is intended or implied. Certain commercial software systems are identified in this paper to facilitate understanding. Such identification does not imply that these software systems are necessarily the best available for the purpose.

References

1. Lechevalier, D., Narayanan A., and Rachuri, S.: Towards a domain-specific framework for predictive analytics in manufacturing. In: 2014 IEEE Conference on Big Data, 2014.
2. Young, M., and Pollard, D.: What businesses can learn from big data and high performance analytics in the manufacturing industry. Big Data Insight Group, 2012.
3. MTConnect: Part 1-Overview and protocol, Version 1.2.0. MTConnect Institute, 2014.
4. Brown, E., and Sturrock, D.: Identifying cost reduction and performance improvement opportunities through simulation. In: Winter Simulation Conference, 2009.
5. Perzyk, M., Biernacki R., and Kochański, A.: Modeling of manufacturing processes by learning systems: The naïve Bayesian classifier versus artificial neural networks. In: Journal of Materials Processing Technology 164: 1430-1435, 2005.3
6. ISO, ISO 14649: 2003, Industrial automation systems and integration - Physical device control - Data model for computerized numerical controllers.
7. Yang, W., and X. Xu.: "Modelling machine tool data in support of STEP-NC based manufacturing." In: International Journal of Computer Integrated Manufacturing, 2008.
8. Vijayaraghavan, Athulan, Sobel, W., Fox, A., Dornfeld, D., & Warndorf, P.: "Improving machine tool interoperability using standardized interface protocols: MT Connect." In: International Symposium on Flexible Automation, 2008.
9. XML, XML Specification available at http://www.w3.org/TR/2008/REC-xml-20081126/.
10. ISO, ISO 6983-1: 1982, Numerical control of machines -- Program format and definition of address words -- Part 1: Data format for positioning, line motion and contouring control systems
11. Avram, O., and Xirouchakis P.: Evaluating the Use Phase Energy Requirements of a Machine Tool System. In: Journal of Cleaner Production 19: 699-711, 2011.
12. Altintas, Y.: Manufacturing Automation: Metal Cutting Mechanics, Machine Tool Vibrations, and CNC Design. Cambridge University Press: Cambridge, 2012.
13. ISO, ISO 10303-1: 1994, Industrial Automation Systems and Integration - Product Data Representation and Exchange -- Part 1: Overview and fundamental principles.
14. Kramer, T. R., Proctor, F., Xu, X., & Michaloski, J. L.: Run-time interpretation of STEP-NC: implementation and performance. In: International Journal of Computer Integrated Manufacturing, Vol. 19, Iss. 6, 2006.
15. Grigoryev, I.. AnyLogic 7 in Three Days: A Quick Course in Simulation Modeling, 2015.
16. Negahban, A., and S. Smith J.: Simulation for manufacturing system design and operation: Literature review and analysis. In: Journal of Manufacturing Systems 33.2: 241-261, 2014.
17. Shao, G., Shin S., and Jain S.: Data analytics using simulation for smart manufacturing. In: Proceedings of the 2014 Winter Simulation Conference. IEEE Press, 2014.

Model-based Engineering for the Integration of Manufacturing Systems with Advanced Analytics

David Lechevalier[1], Anantha Narayanan[2], Sudarsan Rachuri[3], Sebti Foufou[4], Y. Tina Lee[5]

[1]Le2i, Université de Bourgogne,
Dijon, France
david_lechevalier@etu.u-bourgogne.fr

[2]University of Maryland,
College Park, MD, USA
anantha@umd.edu

[3]Office of Energy Efficiency and
Renewable Energy, Advanced
Manufacturing Office, Department of
Energy, Washington, DC, USA
sudarsan.rachuri@hq.doe.gov
sudarsan.rachuri@ee.doe.gov

[4]CSE Department, College of
Engineering,
Qatar University, Qatar
sfoufou@qu.edu.qa

[5]Systems Integration Division, National
Institute of Standards and Technology,
Gaithersburg, MD, USA
yung-tsun.lee@nist.gov

Abstract. To employ data analytics effectively and efficiently on manufacturing systems, engineers and data scientists need to collaborate closely to bring their domain knowledge together. In this paper, we introduce a domain-specific modeling approach to integrate a manufacturing system model with advanced analytics, in particular neural networks, to model predictions. Our approach combines a set of meta-models and transformation rules based on the domain knowledge of manufacturing engineers and data scientists. Our approach uses a model of a manufacturing process and its associated data as inputs, and generates a trained neural network model as an output to predict a quantity of interest. This paper presents the domain-specific knowledge that the approach should employ, the formal workflow of the approach, and a milling process use case to illustrate the proposed approach. We also discuss potential extensions of the approach.

Keywords: Data analytics, meta-model, neural network, manufacturing process, predictive modeling

1 Introduction

The manufacturing industry generates large amounts of data on products, processes, and resources, among other things. Data analytics provide the capabilities needed to extract insights and make predictions from these data. The potential impacts of data analytics on manufacturing-systems efficiency include a reduction of production cost and time across all manufacturing levels [1, 2]. Data scientists and manufacturing engineers often collaborate when using data analytics to solve process-specific problems to improve product quality [3, 4], equipment efficiency [5, 6], and resource

Lechevalier, David; Narayanan, Anantha Narayanan; Rachuri, Sudarsan; Foufou, Sebti; Lee, Yung-T.
"Model-based engineering for the integration of manufacturing system with advanced analytics."
Paper presented at the 13th IFIP International Conference on Product Lifecycle Management (PLM16), Columbia, SC, Jul 11-Jul 13, 2016.

efficiency [7, 8]. However, these collaborations require a significant amount of time and effort to merge the expertise from these two domains. In [9], the authors present a domain-specific framework to address this challenge. The framework 1) identifies the main components and interfaces that must be implemented to improve communication between these domains and 2) facilitates the application of data analytics in manufacturing. In this paper, we introduce an implementation of some of the components and interfaces that will be a part of this framework.

Our approach focuses on using data analytics – specifically neural networks (NNs) – for predicting a set of manufacturing-process-related performance metrics. There are three main contributions of this paper. First, we provide meta-models to represent manufacturing processes and NNs. Second, we describe an algorithm to generate a trained NN automatically from a manufacturing process model and data. Third, we discuss a tool to export the NN in two standard formats: the Predictive Model Markup Language (PMML) [10] and the Portable Format for Analytics (PFA) [11].

The paper is organized as follows. Section 2 presents the domain-specific knowledge required from the manufacturing and data-science domains to generate NNs for manufacturing processes. It also introduces the approach to generate NNs automatically. Section 3 describes, in more detail, two components of the proposed approach: a manufacturing meta-model and transformation rules to generate an NN. Section 4 presents a process-level manufacturing use case to illustrate the capabilities of the approach.

2 Domain Specific Knowledge from Neural Networks and Manufacturing Processes

In this section, we discuss the knowledge required from manufacturing engineers and data scientists to apply NNs to manufacturing processes. We review applications of NNs in manufacturing processes, and devise a methodology based on the common practice of data scientists.

2.1 Manufacturing Domain Knowledge

To identify the required manufacturing-domain knowledge, we studied several research efforts on the applications of data analytics (DA) to manufacturing processes. In [12], the authors apply analytics to detect faults in the alignment of a cap to the base part of a product. In [13], [14], and [15], the authors predict product quality using three DA algorithms: Bayesian networks (BNs), linear regression, and NNs. In [16], the authors describe a way to predict the need for equipment repair using BNs. In [15], the authors used NNs to study surface roughness in a milling process. They identified surface roughness as the performance metric of interest. They also identified spindle speed, feed rate, depth of cut, and the vibration average per revolution as the process variables that have the most impact on surface roughness. They collected 492 data samples to train and validate the NN. Each application followed a similar workflow: 1) identify the performance metric to be studied, 2) identify the variables that impact this target quantity, and 3) use test data to build an analytical model to predict the performance metric from the process variables. We used this same workflow in our work.

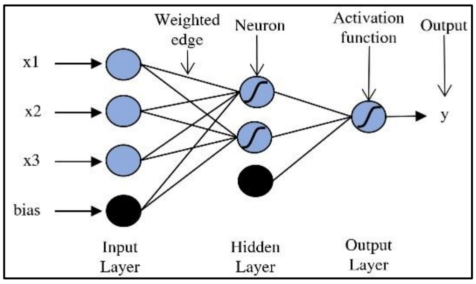


Figure 1. Structure of a Neural Network

2.2 Data Science Domain Knowledge

To understand the knowledge required from a data scientist to apply data analytics techniques to build an NN, it is important to understand how an NN is built. **Figure 1** presents the main elements and the structure of an NN. An NN is composed of an input layer, zero or more hidden layers, and an output layer. Each layer contains at least one neuron. All layers except the output layer contain a bias neuron (shown in black). Weighted edges fully connect neurons in different layers. From a mathematical viewpoint, NNs can be viewed as a set of nonlinear basis functions (the activation functions), with free parameters (the adjustable weights). Training the NN is about adjusting the weights to minimize the error between the output value of the NN and the known, real, output value for a given data sample [17].

As noted above, the first step in building the NN involves selecting the input variables relevant to the performance metric. This step is called *feature selection* and defines the number of input neurons of the NN. There is one input neuron for each input variable. The second step is to determine the number of hidden layers and the number of neurons in each layer. In general, one hidden layer is sufficient [18] for the class of problems related to manufacturing processes. The number of hidden neurons has an impact on the NN accuracy, thus data scientists define this number very carefully. Finally, the output neuron represents the variable that we are trying to predict, which we call the quantity of interest. For example, a performance metric such as energy consumption may be the quantity of interest in a manufacturing scenario.

Based on these reviews, our approach needs to define the input neurons based on the process variables, define the optimal number of hidden neurons for an NN with one hidden layer, and finally define the output neuron for the quantity of interest.

2.3 Integration of Manufacturing and Data Science Domain Models

After identifying the required knowledge from manufacturing engineers and data scientists, we describe our approach and how it contributes to the framework defined in [9]**. Figure 2** summarizes the workflow of our approach. In this figure, meta-models (Ⓐ and Ⓑ) are in gray, models (①, ③ and ⑤) are in yellow, and software solutions (②, ④ and ⑥) are in blue. The dashed arrows represent actions defined in the related label. The solid arrows show the use of models as input or output of the software solutions.

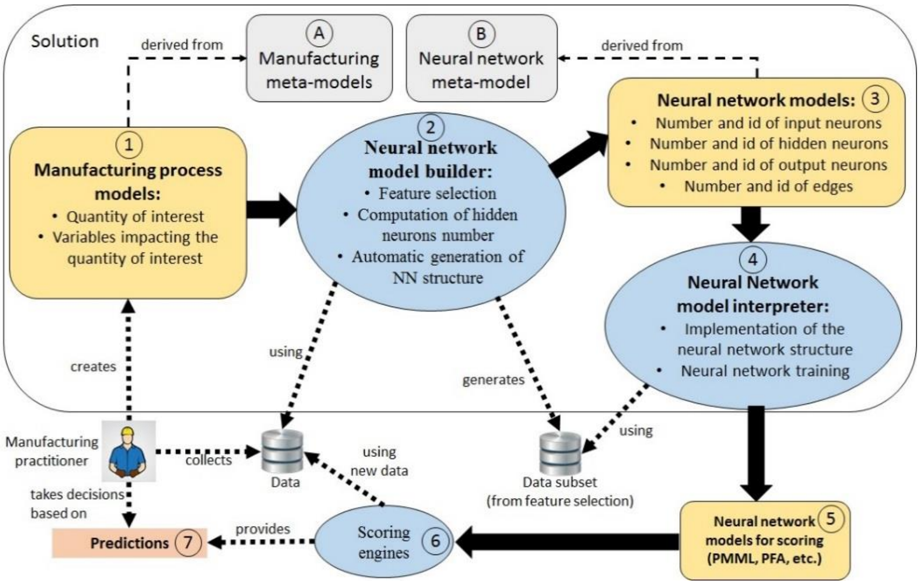

Solution
derived from
Ⓐ Manufacturing meta-models
Ⓑ Neural network meta-model
derived from
① Manufacturing process models:
• Quantity of interest
• Variables impacting the quantity of interest
② Neural network model builder:
• Feature selection
• Computation of hidden neurons number
• Automatic generation of NN structure
Neural network models: ③
• Number and id of input neurons
• Number and id of hidden neurons
• Number and id of output neurons
• Number and id of edges
④ Neural Network model interpreter:
• Implementation of the neural network structure
• Neural network training
creates
using
generates
using
Manufacturing practitioner
collects
Data
using new data
Data subset (from feature selection)
takes decisions based on
Predictions ⑦
provides
Scoring engines ⑥
Neural network ⑤ models for scoring (PMML, PFA, etc.)

Figure 2. Formal workflow of the approach

Box Ⓐ represents our manufacturing meta-model that captures the manufacturing knowledge. This meta-model defines the concepts, rules and constraints needed to represent a manufacturing process. Using the meta-model, a manufacturing engineer is able to build a manufacturing process model ① to define the quantities of interest and the variables involved in the manufacturing process. Note, we provide an interface to collect data related to the manufacturing process.

Taking the manufacturing process model and data as inputs, an NN model builder ② embeds a set of algorithms to run a feature selection that 1) optimizes the number of input neurons, 2) computes the optimal number of hidden neurons, and 3) builds the optimal structure of the NN ③. This NN structure is recorded using an NN meta-model contained in the meta-model repository. The NN meta-model and NN model interpreter are presented in [19]. The NN model interpreter ④ generates a trained NN. This NN is exported as a PMML or PFA file ⑤ that is ready to use for prediction with new data. A scoring engine ⑥ provides predictions ⑦ using the PMML file and new data. Scoring is the process of using a model to make predictions about the behavior of a quantity of interest. A manufacturing engineer makes decisions based on these predictions to control the manufacturing process under investigation.

3 Manufacturing Meta-Models and Transformation Rules of the Neural Network Builder

In this section, we describe the components, Ⓐ, Ⓑ and ② in **Figure 2**, to generate NNs from manufacturing process descriptions automatically. We also describe our implementations of these components.

3.1 Meta-Model for Manufacturing Processes

A meta-model is a graphical description of concepts and their relationships, which can be used to describe objects or instances of those concepts in a particular domain. We developed a meta-model for describing manufacturing processes in a way that is helpful to build an NN. A manufacturing engineer builds a manufacturing model using the meta-model to provide the required knowledge identified in Section **2.1**. Since the purpose of the approach is to use data-driven techniques (in this case NNs), there are no physics-based equations associated with the model. **Figure 3** presents the main concepts of the manufacturing meta-model. Please note that this is a simple but a reasonable representation of the domain model. The notation in **Figure 3** and **Figure 4** is based on Unified Modeling Language Class Diagrams [20], where the rectangles represent concepts occurring in the domain, and the lines represent relationships between the concepts. A line with a solid diamond represents a containment relationship, with a numerical range at one end denoting the number of allowed instances. For example, in **Figure 3**, a *ManufacturingModel* can contain 0 or more instances of *ManufacturingProcess*.

The annotation <<Model>> is used to identify first class objects, while the annotation <<Connection>> is used to represent edges, flows, or associations. *ManufacturingModel* is a high level concept that allows the description of a manufacturing model that is composed of *Flows* and *ManufacturingProcess* concepts.

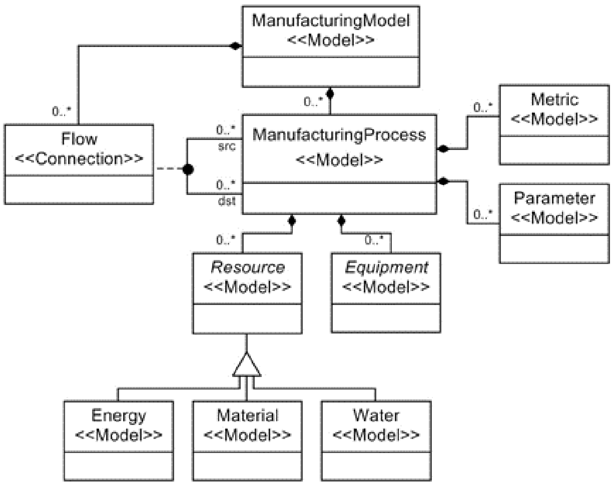


Figure 3. Manufacturing meta-model

The *Flow* concept represents connections between instances of the *ManufacturingProcess* concept. A *ManufacturingProcess* is composed of *Resource* and *Equipment* concepts, which allow the manufacturer to include resource or equipment parameters as variables of the manufacturing process. *ManufacturingProcess* also contains the concepts of *Parameter* and *Metric*. Metric is used to define a quantity of interest in the manufacturing process. Parameters are the variables that can impact the metric for a manufacturing process.

In the UML notation, an empty triangle is used to denote specialization, where one concept may be specialized into many sub-concepts. As shown in **Figure 3**, the *Resource* concept is extended to define different types of resources: energy, water, and material. The manufacturing meta-model can also be extended to define other kinds of resources such as labor.

3.2 Meta-Model for Neural Networks

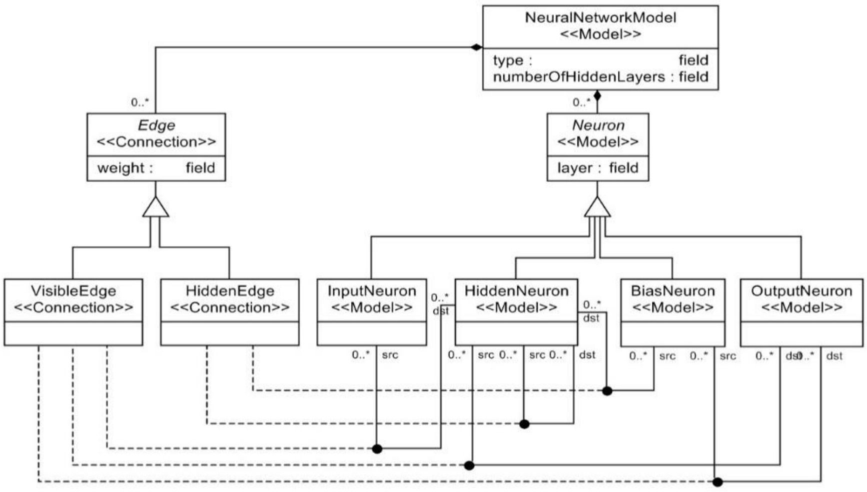


Figure 4. Neural network meta-model [19]

Figure 4 shows the neural network meta-model (NNMM) presented in [19]. The NNMM represents different types of NNs through various abstractions. A *NeuralNetworkModel* concept is composed of *Neuron* and *Edge* concepts. A *Neuron* can be one of four types: *InputNeuron*, *HiddenNeuron*, *BiasNeuron*, and *OutputNeuron*. An *Edge* can be a *VisibleEdge* or a *HiddenEdge*. A *VisibleEdge* is used to represent an edge between an input neuron and a hidden neuron, between a hidden neuron and an output neuron, or between a bias neuron and an output neuron. Edges between two hidden neurons, or between a bias neuron and a hidden neuron are represented using *HiddenEdge*.

3.3 Transformation Rules to Generate an NN from a Manufacturing Model

We developed a set of transformation rules to generate an NN model from a manufacturing model. Together, these rules represent a step-by-step process to build an NN from the input model and the data provided by a manufacturing engineer. We embedded these rules into the NN model builder, so that they can be applied to any type of manufacturing process model. The result of applying these rules is an untrained NN model, which is built based from the NN meta-model described above, and an input data set for training. **Figure 5** presents the workflow and the transformation rules of the NN model builder, identified as ② in **Figure 2**.

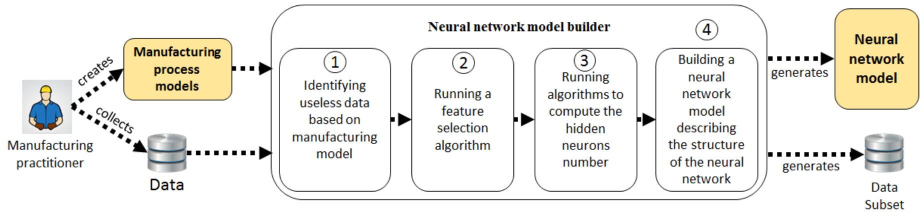

Neural network model builder
Manufacturing process models
creates
collects
Manufacturing practitioner
Data
1
Identifying useless data based on manufacturing model
2
Running a feature selection algorithm
3
Running algorithms to compute the hidden neurons number
4
Building a neural network model describing the structure of the neural network
generates
Neural network model
generates
Data Subset

Figure 5. Workflow of the NN model builder

The NN model builder takes the manufacturing process model and data provided by the manufacturing engineer as inputs. In the builder, Step 1 identifies those variables that the manufacturer listed as impacting the quantity of interest in the manufacturing model. The identified variables are compared with the variables present in the data set. The variables that are not identified in the manufacturing model are then removed. Step 1 takes advantage of the manufacturing expertise that the manufacturing engineer provides in the model.

Step 2 uses the feature-selection algorithm and a real data set to identify those variables that do not contribute to the quantity of interest based on a data set. This algorithm takes the variables provided from Step 1 and removes the variables that do not contribute from the list.

During Step 3, the builder runs an algorithm to optimize the number of hidden neurons for the NN. Several reports document the studies associated with optimizing the number of hidden neurons and putting them all into a single hidden layer. Sheela et al. [21], for example, analyzes the performance of the different optimization methods described in different reports – that is, their ability to predict the actual optimal number of hidden neurons. Our algorithm applies these different methods and computes the number that appeared most frequently. That number is the one selected for the NN. As we mentioned previously, one hidden layer is sufficient for manufacturing process-related problems, and the algorithm is implemented to build one hidden layer. This algorithm, however, can easily be modified to build NNs with more than one hidden layer.

In Step 4, the builder generates the NN instance model and a data set as outputs. The NN instance model describes the structure of the NN, and must be trained in order to predict the quantity of interest. The output data set is a subset of the input data set. The input data set variables that do not impact the quantity of interest are not included in the output data set.

Using the output data set, the NN model interpreter [19] performs the NN training and updates the weights on the NN instance model. It also generates a PMML or PFA file containing the trained NN model.

4 Use Case

In this section, we show how our implementation of the proposed approach is used in a typical manufacturing scenario. For our approach, manufacturing engineers build a model of the process they wish to study using the meta-model described earlier. Next, they collect test data by conducting experiments or from other sources. Finally, they use the automated tools described in **Figure 2** to generate an NN for their process. This NN can be used to make future decisions without having to conduct physical experiments to determine target values.

4.1 Scenario Description

This case study focuses on predicting the energy consumed by a milling machine tool. The data set used in this case study was generated in [22] from a total of 18 parts machined with 196 face milling, 108 contouring, 54 slotting and pocketing, 16 spiraling and 32 drilling operations. We focused on face milling in this use case. The series of machining operations were performed. Data was collected using power meters and different sensors, and then stored in a database. We use the collected data as test data to build an NN model to predict power consumption for different combinations of machining parameters.

The test data includes the timestamp, power demand, feed rate, spindle speed, depth of cut, cutting direction, cutting strategy, cutting ratio, cutting volume, and length of cut in the 3 axis, referred as cutX, cutY and cutZ. As described below, we first built a manufacturing process model based on our case study, then identified the optimal process parameters and the metric of interest.

4.2 Building the Manufacturing Process Model

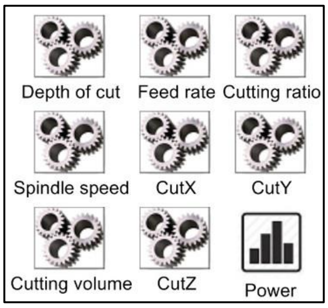


Figure 6. Manufacturing model

Figure 6 shows the manufacturing process model that we built for the milling process. This model contains the parameters that the manufacturing engineer has specified as contributing to the quantity of interest. In this model, we defined power as the quantity of interest. We defined feed rate, spindle speed, depth of cut, cutting ratio, cutting volume, cutX, cutY, and cutZ as parameters that impact the power consumption. During this step, the manufacturers use their domain expertise to list only those parameters that they think will have a significant impact on their power consumption. The test data and the manufacturing model are the inputs to our next step, which performs feature selection and generates the NN.

4.3 Generating the Neural Network for Prediction

In the next step, the manufacturing engineer executes the NN model builder using both the manufacturing model (in **Figure 6**) and the test data as inputs. Our algorithm, takes those inputs and generates a trained NN. It does this using two pieces of software: the NN model builder and the NN model interpreter.

The NN model builder identifies the quantity of interest (the selected performance metric) from the manufacturing model. In this case, it is power. The NN model builder prunes the data set by removing the data that were omitted in the manufacturing model. In our case, it removes the cutting direction and cutting strategy variables from the data set since these are not present in the manufacturing model in **Figure 6**. Next, the feature selection algorithm is executed. It uses the test data to identify and remove parameters that have an insignificant impact on the target variable. In our example, feed rate, depth of cut, cutX, and cutY were found not to have a significant effect on power; therefore, these parameters are not considered when building the NN.

The NN model builder then displays which variables were removed 1) based on the manufacturing model and 2) using the feature selection algorithm. Then the builder saves the new data set in a location identified by the manufacturing engineer. **Figure 7** shows the resulting NN model, an automatically generated instance of the NNMM which is shown in **Figure 4**.

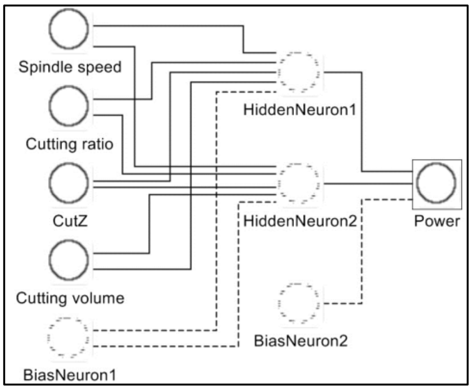


Figure 7. Neural network model

In this NN model, the NN model builder keeps four variables: spindle speed, cutting ratio, cutting volume and cutZ. They are defined as input neurons in the NN. The algorithm computes that two hidden neurons are optimal in this model. Power is defined as the output neuron in the NN. Finally, the builder adds a bias neuron for every layer except the output layer to build a correct NN.

The NN model builder generates the structure model the NN. It still needs to be trained (i.e. weights must be assigned to the edges to make correct predictions). To generate the weights, the structural NN must be trained with the test data. The NN model and the test data are inputs to the NN model interpreter. The interpreter generates a trained NN based on the structure described in the NN model and the test data. The NN is generated as a standard PMML file. Several off-the-shelf data analytics tools can read this PMML file.

The manufacturer can now use this NN to predict the energy consumption of the milling machine under different conditions. This allows the manufacturer to perform different tests and make decisions, without having to physically execute experiments on the machine.

5 Summary and Future Work

In this paper, we proposed an approach to generate an NN to predict performance metrics for manufacturing processes. This approach provides capabilities to collect the required manufacturing knowledge and to use that knowledge to build NN models to predict the performance metrics for different values of the process parameters. This can be used to optimize performance by finding the best values for the process parameters.

We first reviewed the applications of data analytics to manufacturing processes for identifying the steps taken by data scientists to create NNs. We then developed and implemented the components needed to provide the capabilities required by this approach. Part of that approach is developing a manufacturing meta-model. The meta-model allows manufacturing engineers to provide a set of the most important process parameters – those have the most impact on performance – in a manufacturing model. In addition to this meta-model, we implemented an NN model builder to automatically build an NN model from a manufacturing model and data provided by manufacturing engineers. The NN model builder provides 1) a feature-selection algorithm based on the test data and 2) an NN model generator that generates the structure of the NN. From the generated NN structure, an NN model interpreter produces a trained NN in a standard format. Using a scoring engine, the trained NN can then be used to predict the quantity of interest.

We illustrated the capabilities of our implementation using a realistic manufacturing scenario. In this scenario, an NN is trained to predict energy use during a particular milling process. A manufacturing engineer provides a manufacturing model used as input to the NN builder. The implemented algorithms finally generate a trained NN that can be used with new data for predicting energy consumption.

This paper presented an initial description and implementation of an approach to generate predictive models for manufacturing applications. We implemented a translator (the NN model builder) to generate neural networks automatically. More translators will be implemented in future work to generate other types of predictive models. In practice, manufacturing processes and their interactions with their surrounding environment are complex. In order to generate reliable prediction models for practical scenarios, our meta-models and translators must be extended to account for other parameters and constraints that affect manufacturing processes. Future work lies in four directions. The first is to extend the manufacturing meta-model to enable the representation of problems in greater detail, and at different manufacturing levels such as assembly. Next, add new steps to the NN model builder to improve its accuracy. Third, include a scoring engine. Fourth, extend the framework to include different analytical techniques such as Bayesian networks. Capabilities to build BN models could enable the application of uncertainty quantification in manufacturing [23].

Acknowledgement

The research in this paper was supported by National Institute of Standards and Technology's Foreign Guest Researcher Program, and Cooperative Agreement No. 70NANB14H250.

References

1. Manyika, James, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela H. Byers. "Big data: The next frontier for innovation, competition, and productivity." (2011).

2. Brown, Brad, Michael Chui, and James Manyika. "Are you ready for the era of 'big data'." McKinsey Quarterly 4, no. 2011 (2011): 24-35.
3. Erzurumlu, Tuncay, and Hasan Oktem. "Comparison of response surface model with neural network in determining the surface quality of moulded parts." Materials & design 28, no. 2 (2007): 459-465.
4. Zhai, Lian-Yin, Li-Pheng Khoo, and Sai-Cheong Fok. "Feature extraction using rough set theory and genetic algorithms—an application for the simplification of product quality evaluation." Computers & Industrial Engineering 43, no. 4 (2002): 661-676.
5. Dabbas, Russ M., and Hung-Nan Chen. "Mining semiconductor manufacturing data for productivity improvement—an integrated relational database approach." Computers in Industry 45, no. 1 (2001): 29-44.
6. Chien, Chen-Fu, Alejandra C. Diaz, and Yu-Bin Lan. "A data mining approach for analyzing semiconductor MES and FDC data to enhance overall usage effectiveness (OUE)." International Journal of Computational Intelligence Systems 7, no. sup2 (2014): 52-65.
7. Shin, Seung-Jun, Jungyub Woo, and Sudarsan Rachuri. "Predictive analytics model for power consumption in manufacturing." Procedia CIRP 15 (2014): 153-158.
8. Gupta, D., and B. Gopalakrishnan. "Energy sensitive machining parameter optimisation." International Journal of Industrial and Systems Engineering 5, no. 4 (2010): 405-423.
9. Lechevalier, David, Anantha Narayanan, and Sudarsan Rachuri. "Towards a domain-specific framework for predictive analytics in manufacturing." In Big Data (Big Data), 2014 IEEE International Conference on, pp. 987-995. IEEE, 2014.
10. PMML v4.2.1, 2016. [Online]. Available: http://dmg.org/pmml/pmml-v4-2-1.html [Accessed: May 1st, 2016].
11. PFA v0.8.1, 2016. [Online]. http://dmg.org/pfa/index.html [Accessed: May 1st, 2016].
12. Wolbrecht, Eric, Bruce D'ambrosio, Robert Paasch, and Doug Kirby. "Monitoring and diagnosis of a multistage manufacturing process using Bayesian networks." Ai Edam 14, no. 01 (2000): 53-67.
13. Correa, M., C. Bielza, M. de J. Ramirez, and J. R. Alique. "A Bayesian network model for surface roughness prediction in the machining process." International Journal of Systems Science 39, no. 12 (2008): 1181-1192.
14. Abouelatta, O. B., and J. Madl. "Surface roughness prediction based on cutting parameters and tool vibrations in turning operations." Journal of materials processing technology 118, no. 1 (2001): 269-277.
15. Tsai, Yu-Hsuan, Joseph C. Chen, and Shi-Jer Lou. "An in-process surface recognition system based on neural networks in end milling cutting operations." International Journal of Machine Tools and Manufacture 39, no. 4 (1999): 583-605.
16. Kurz, Daniel, Johannes Kaspar, and Jürgen Pilz. "Dynamic maintenance in semiconductor manufacturing using Bayesian networks." In Automation Science and Engineering (CASE), 2011 IEEE Conference on, pp. 238-243. IEEE, 2011.
17. Haykin, S. "Neural Network A comprehensive foundation." Neural Networks 2, no. 2004.
18. Heaton, Jeff. "Introduction to neural networks with Java." Heaton Research, Inc., 2008.
19. Lechevalier, David, Steven Hudak, Ronay Ak, Y. Tina Lee, and Sebti Foufou. "A neural network meta-model and its application for manufacturing." In Big Data (Big Data), 2015 IEEE International Conference on, pp. 1428-1435. IEEE, 2015.
20. Unified Modeling Language [Online]. http://www.uml.org [Accessed: May 1st, 2016].
21. Sheela, K. Gnana, and S. N. Deepa. "Review on methods to fix number of hidden neurons in neural networks." Mathematical Problems in Engineering 2013 (2013).
22. Park, Jinkyoo, et al. "A generalized data-driven energy prediction model with uncertainty for a milling machine tool using Gaussian Process." ASME 2015 International Manufacturing Science and Engineering Conference, 2015.
23. Nannapaneni, Saideep, and Sankaran Mahadevan. "Uncertainty quantification in performance evaluation of manufacturing processes." Big Data (Big Data), 2014 IEEE International Conference on. IEEE, 2014.

Design and calibration of an artifact for evaluating laser scanning articulating arm CMMs used for measuring complex non-concurrent surfaces

Vincent D. Lee[1], Steven D. Phillips[1], Craig M. Shakarji[1],
Jeffrey J. Hosto[2], Jeffrey M. Huber[2], and Barbara J. Gillich[2]
[1]Dimensional Metrology Group
National Institute of Standards and Technology
Gaithersburg, Maryland
[2]Protective Equipment Division
US Army Aberdeen Test Center
Aberdeen, Maryland

INTRODUCTION

Laser scanners mounted to articulated arm coordinate measuring machines (LS/AACMM) have been recently adopted by the US Army to evaluate ballistic threat mitigation capabilities of human worn body armor. In brief, testing of the armor is performed by placing the article under test against a clay substrate (pre-impact surface), that has been shaped to conform to the concave surface of the body armor, and firing a projectile of a known mass, shape and velocity at it. When the projectile strikes the armor, its kinetic energy is transferred into the armor and clay, resulting in an impact crater (post-impact surface) into the clay known as a back face deformation (BFD), and is an indication of the blunt-force trauma a wearer would experience. The maximum depth of the BFD is used as part of an evaluation criterion to determine if a batch of armor would be placed into service or rejected.

In the past, the measurand of the BFD was defined as the distance between the pre-impact surface, and the post-impact surface, at the point of aim, known as the "*Basic Length"* FIGURE 1*.* This measurement was carried out with a measurement device that was similar to a depth gauge called a bridge caliper (BC). With the BC the operator would measure the height of the clay at the point of aim for the projectile, followed by a measurement of the depth at this same point in the impact crater; this method yielded expanded $(k = 2)$ measurement uncertainties ranging from 1.6 mm to 1.9 mm, more details can be found in [1, 2]. Among the complications of the BC method is that the BFD at the point of aim—which is a point on the pre-impact surface identified by the laser sight—is not necessarily the maximum BFD depth; see FIGURE 1.

A significant metrological improvement to the BFD measurement process was the introduction of LS/AACMM technology. This allowed the measurand to be unambiguously defined as the longest line segment measured between the pre-impact surface and post-impact surface, known as the "*Maximum Distance Length*"; see FIGURE 1. Using the LS/ASCMM removed the

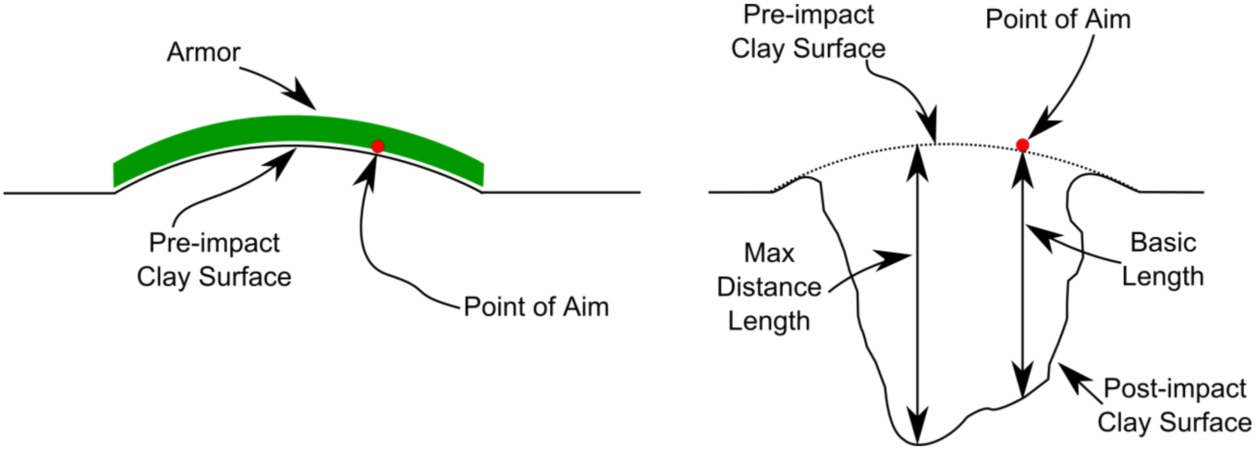


FIGURE 1: (Left) Arangement of the armor over clay, (Right) Example of impact crater in clay with resprect to pre-impact surface

problematic issue that the point of aim did not necessarily correspond to the point of maximum depth length. Since the location of this maximum value is not known until the post-impact surface is created—and hence the pre-impact surface obliterated—the manual BC method is ineffective in determining the maximum depth length measurand, because detailed topography of the pre-impact surface is required prior to the post-impact surface creation. The LS/AACMM can scan and store detailed information about the pre-impact surface, so it can be recalled and compared against the post-impact surface to calculate the maximum distance length. The initial implementation of the LS/AACMM system significantly reduced the maximum distance length expanded $(k = 2)$ uncertainty to 0.37 mm for typical BFD values.

In order for the LS/AACMM system to calculate the BFD value correctly, the pre and post-impact surfaces need to be recorded in a common coordinate system so that the two surfaces can be registered correctly with respect to each other. Three coplanar conical seats on the clay's container provide an interface for the hard probe on the LS/AACMM to establish three discrete points to establish a common datum reference frame (DRF) for both data sets; see FIGURE 3, FIGURE 3, & FIGURE 4.

In brief, the evaluation and measurement of a BFD value is as follows:

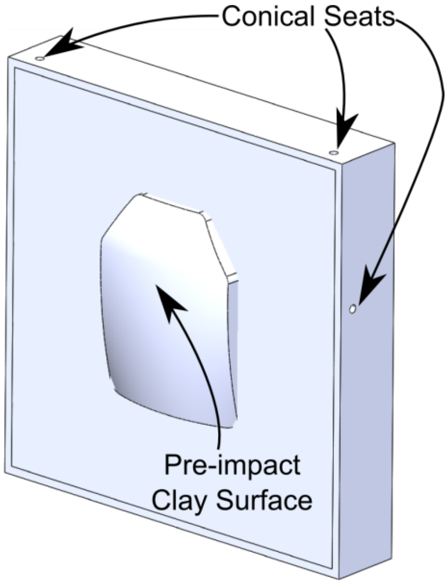


FIGURE 2: Location of conical seats on box relative to pre-impact surface

1) A DRF is established by measuring the conical seats on the box using the hard probe of the LS/AACMM.
2) The pre-impact surface is scanned and recorded using the LS/AACMM.
3) The body armor plate is attached on top of the clay surface.
4) A rifle round is fired into the armor and the armor is removed
5) The DRF is established again by measuring the conical seats on the box using the hard probe of the LS/AACMM.
6) The post-impact surface is measured using the LS/AACMM.
7) Mathematical software uses the pre- and post-impact scan data to calculate the maximum BFD distance as defined by Army specifications.

As part of a continuous improvement process, the US Army requested from NIST a measurement check standard to evaluate the performance of the LS/AACMM *in situ* on the live fire test ranges. NIST designed two working prototypes; this paper discusses their designs.

DESIGN OF TEST ARTIFACTS

To adequately test the LS/AACMM used by the Army, the following core design requirements were outlined for the artifacts.

1. Needs to be metrologically traceable
2. A BFD maximum-distance value uncertainty ≤ 0.090 mm (1/4 of initial LS/AACMM measurement uncertainty)
3. Dimensionally stable (less than 0.010 mm per year, for BFD)
4. Contain dimensional features that represent those encountered during measurement
5. Surface features that exercise software for BFD evaluation
6. Similar reflective properties of the backing clay
7. Contain a feature to represent a typical pre-impact test surface
8. Contain a feature(s) to represent a post-impact test surface
9. Contain features used to register pre and post impact scanned data
10. Mimic the BFD measurement work flow.

Considering these design requirements, several design concepts where conceived with two of them developed as prototypes for testing, calibration and delivery to the US Army for further evaluation, and deployment in their testing facilities.

Design of Concept 1: Kinematic Design

The first design concept consists of two kinematically coupled parts, one representing the pre-impact surface and the other representing the post-impact test surface. The pre-impact surface is modeled after a partial cylindrical section, while the post-impact surface is freeform in nature and modeled after an actual BFD test shot. The test shot chosen by the US Army contains features that display fine structure and sharp changes in gradient that are believed to adequately challenge the LS/AACMM system. These two test surfaces are located and connected together using a kinematic coupling, superimposing one test surface over the other, mimicking how their clay counterparts would be positioned in an actual test (FIGURE 3). The kinematic coupling is a key feature in providing repeatable location of the two parts on the order of *1* µm [3], thus maintaining the calibration between the two parts. This assembly is then mounted into a container that resembles a clay container used in live fire testing. It also contains three coplanar conical seats for the hard probe of the LS/AACMM to establish a datum reference frame (DRF) for each surface. Calibration of this concept would follow the same work flow as measuring a BFD value during live testing by the Army. First, the centers of the three conical seats are measured to establish a DRF. Next, the part representing the pre-impact surface is scanned. Then the pre-impact surface is removed, exposing the post-impact surface. Finally, the conical seats are measured again, and the post-impact surface is scanned.

Design of Concept 2: Dual Chamber Design

The second design concept is functionally similar to the previous one, but rather than have the pre-impact surface physically superimposed over the post-impact surface, the two surfaces are contained in their own chambers with their own DRFs. Since the DRF has to be established before a scan is performed, each surface can be scanned independently as long as the DRF associated with that surface is used. The software will automatically superimpose the pre-impact surface over the post-impact surface to calculate the BFD.

The surfaces for both of these design concepts have been media blasted using 400 grit aluminum oxide powder to provide a surface finish that is cooperative with the LS/AACMM system, and similar to the clay surface.

CALIBRATION OF TEST ARTIFACTS

Calibration of these artifacts was performed on a high accuracy Leitz PMM-C 8.10.6 coordinate measurement machine with a tactile touch probe. A stylus with a 0.5 mm diameter tip was used to probe the fine structure of the post-impact surface, which was milled using a 0.0625 inch diameter ball nose end mill. To adequately digitize the surfaces a point measurement density of 20 points per mm was used. However the area which the BFD could potentially be located in spans 30 x 30 mm. Measuring this area using a high point density would be time consuming and impractical. The solution was to use a course measurement to identify a few candidate locations that could possibly contain

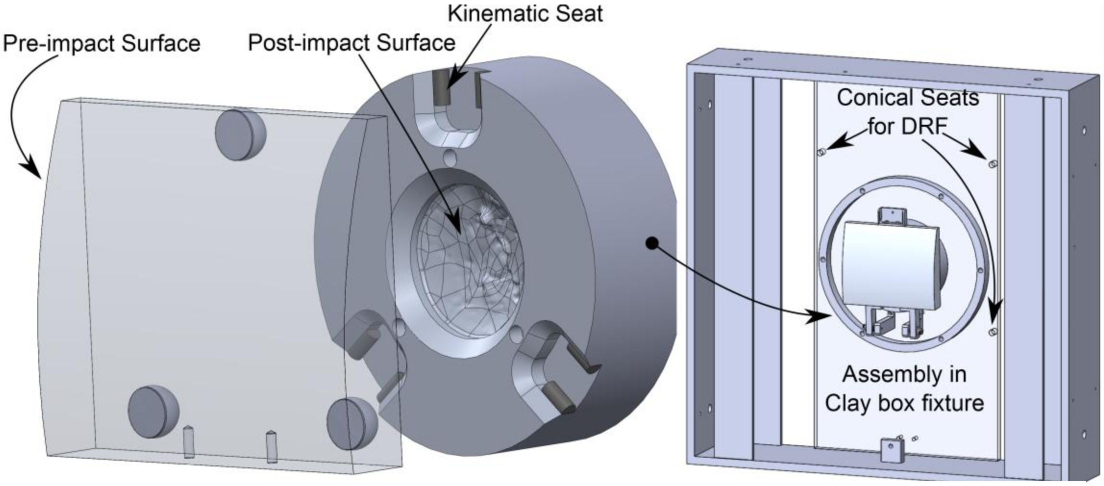


FIGURE 3: (Left) Detailed view of Kinematic design, (Right) Position of artifact in box fixture

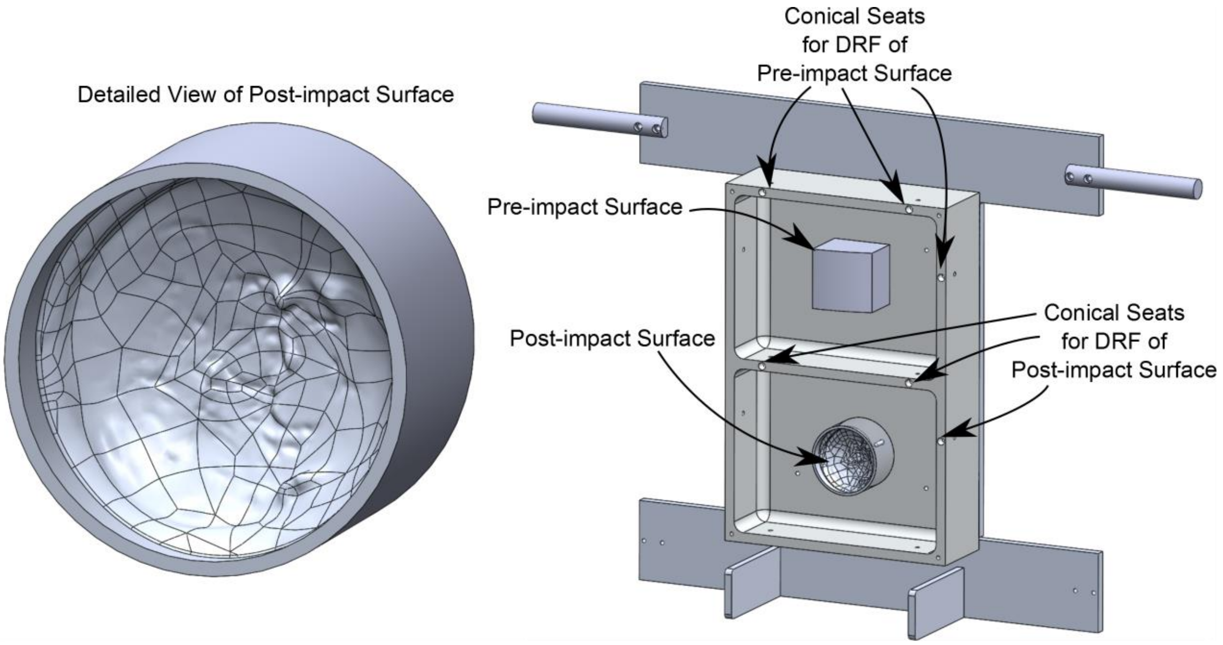

Detailed View of Post-impact Surface
Conical Seats for DRF of Pre-impact Surface
Pre-impact Surface
Post-impact Surface
Conical Seats for DRF of Post-impact Surface

FIGURE 4: (Left) Detailed view of Post-impact surface for Dual Chamber design, (Right) Assembly of pre and post-impact surfaces in dual chamber fixture with respect to DRFs

the largest BFD value and then measure those few locations with a high point density. These artifacts were placed in the CMM such that the surfaces being measured were approximately perpendicular to the *Z* axis of the machine.

The data collected was post-processed by NIST's own mathematical software algorithms, and not the proprietary software used by the Army, allowing an independent check even of the software processing/smoothing algorithms used during actual BFD testing.

CALIBRATION UNCERTAINTY and RESULTS

The data captured by the CMM was post processed using an NIST algorithm designed to yield the value of the maximum distance length measurand [1]. The calibrated BFD values for the two artifacts described in this paper are outlined in *Table 1*. The NIST measurement uncertainty budget for the kinematic design (KD) and the dual chamber (DC) design are shown in Table 2. The expanded uncertainties are 18 % and 27 % of the initial design target uncertainty of 90 µm, respectively.

Table 1: Calibration results for kinematic deign (KD) and dual chamber (DC) BFD artifacts (mm)

	BFD Value	Uncertainty (*k=2*)
Design 1 (KD)	47.704	0.016
Design 2 (DC)	41.240	0.024

Table 2: NIST measurement uncertainty budget

	KD std. unc. (µm)	DC std. unc. (µm)
Local CMM repeatability on pre- & post- impact surfaces	0.3	0.6
Projection of coordinates from stylus center to BFD surface	4.9	4.9
Z-axis systematic errors from calibrated step standards	0.1	0.1
Coordinate system and kinematic reproducibility	4.2	6
Thermal uncertainties: Due to Uncertainty in Temperature Due to Uncertainty in CTE	 < 0.1 < 0.1	 < 0.1 < 0.1
BFD algorithm accuracy	< 0.1	< 0.1
Loading deformation on BFD	5.1	9.0
Combined standard uncertainty	8.2	12
Expanded uncertainty (*k* = 2)	16	24

ARMY TESTING RESULTS

Initial testing results conducted at the Army's Aberdeen Test Center (ATC) are summarized in Table 3. The measurements consist of 48 BFD values (from eight different technicians) performed both in ATC's laboratory, using equipment and procedures similar to the live-fire test ranges, and on the actual live-fire test ranges. Examination of the estimated errors (each error being the ATC measured value minus the NIST calibrated value) provides insight into the effectiveness of the BFD artifacts and an initial view of ATC's current measurement capability. Table 3 shows a summary of the results, presented as (1) the 95th percentile of the error distribution and (2) twice the root-mean-square of the estimated errors. The RMS value was computed, as opposed to the standard deviation, because the RMS evaluates deviations from the calibrated value including systematic errors, as opposed to just the deviations from the mean error, which are evaluated in the standard deviation. A complete ATC uncertainty budget would require more measurements spanning a wider range of influence quantities and also combining the NIST calibration uncertainty. Nonetheless the currently available ATC results show excellent agreement with the NIST calibrated values, especially notable in consideration of the high-volume measurement environment of the actual test ranges. The significant improvement in ATC's measurement capability reflects an ongoing effort for continuous metrological improvement of their BFD dimensional measurement capability.

Table 3: Initial ATC test results: 2 RMS and 95th percentile* of (ATC value – NIST value) (mm)

	KD 2*RMS	KD 95th %	DC 2 *RMS	DC 95th %
ATC Lab	0.040	0.047	0.037	0.039
ATC Live Fire Range	0.063	0.060	0.109	0.094

CONCLUSION

Two artifacts satisfying all of the core design requirements have been designed, developed, calibrated, and delivered to the US Army. Feedback from the Army noted that both designs performed well with their LS/AACMM systems. The kinematic design provided more repeatable results when measured in ATC's live fire range, when compared to the dual chamber concept. One likely reason is that the pre and post-impact surfaces share a common DRF. The other is the short metrological loop that is maintained by the kinematic coupling of the pre and post-impact surfaces. However the kinematic design was very sensitive to incomplete seating of the kinematic coupling. If the not properly seated, the kinematic design would produce an incorrect BFD value, something that the dual chamber design wasn't' subjected to since it has no moving parts. . Comparison with an initial set of Army BFD measurements shows excellent agreement with NIST results and significant metrological improvements relative to their initial implementation of the LS/AACMM system.

DISCALIMER

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the test and measurement procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

REFERENCES

[1] K. Rice, M. Riley, A. Forster, S. D. Phillips, C. M. Shakarji, D. Sawyer, *et al.*, "Dimensional Metrology Issues of Army Body Armor Testing," National Institute of Standards and Technology, Gaithersburg, MD 2010 (unpublished).

[2] "Department of Defense Test Method Standard For Performance Requirements and Testing of Body Armor," in *MIL-STD-3027*, ed: Department of Defense, 2008.

[3] A. Slocum, *Precision Machine Design*. Dearborn, Michigan: Society of Manufacturing Engineers, 1992.

Towards Estimating the Uncertainty Associated with 3D Geometry Reconstructions from Medical Image Data

[1]Marc Horner, [2]Kerim O. Genc, [3]Stephen M. Luke, [4]Todd M. Pietila, [3]Ross T. Cotton, [5]Benjamin A. Ache, [6]Zachary H. Levine, [4]Kevin C. Townsend and [3]Philippe G. Young
[1]ANSYS, Inc., Evanston, IL, [2]Simpleware Inc., Herndon, VA. [3]Simpleware Ltd., Exeter, UK, [4]Materialise, Plymouth, MI, [5]Micro Photonics, Inc., Allentown, PA, [6]National Institute of Standards and Technology (NIST), Gaithersburg, MD.

3D-image based geometries are increasingly used for patient-specific visualization, measurement, physics-based simulation and additive manufacturing. Computed Tomography (CT) is a common imaging modality used to obtain the 3D geometry of objects through X-ray images taken from different angles to produce cross-sectional images along an axis. Levine *et al.* (1,2) developed a reference phantom, or "NIST phantom", to help control for variations in scanner settings, noise and artifacts. Ideally, the geometry of the phantom would be extracted through the ISO 50 standard threshold-based segmentation, which states that the material boundary is set as the middle greyscale value between the background and material peaks in the greyscale value histogram (3). The purpose of this study is to examine the effects of image resolution on the uncertainty associated with 3D geometries reconstructed from idealized and real CT images.

An idealized spherical reference phantom of known diameter was generated in CAD format used by AutoCAD. A CAD voxelization process was used to convert the CAD sphere into 3D greyscale images at various resolutions. These images were then used to study the effect of image resolution on measurement accuracy of the sphere diameter, measured via a sphere-fitting method. Next, an image stack of the NIST phantom, generated using a SkyScan 1173 CT scanner (Bruker MicroCT N.V. Kontich, Belgium), was resampled to various resolutions to allow for a similar accuracy study. Image stacks generated from the voxelized CAD sphere were devoid of artifacts, and as such, an ISO50 thresholding approach could be used with confidence. A similar ISO50 technique was also applied to the segmentation of the NIST phantom data.

During the CAD sphere voxelization process, the accuracy of measurement was 2% if 5 or more voxels were present across the sphere diameter. The measurement accuracy degraded to approximately 4% for a similar degree of voxelization when resampling the CT scan data of the NIST phantom. The main source of this inaccuracy appears to be related to the choice of segmentation threshold. Investigation of threshold choice suggests the ISO50 segmentation approach is not suitable for these CT images, which is in agreement with results in published literature (3).

Through an idealized image set (i.e. a perfect CT scan), we have shown that a measurement accuracy of 2% or less can be maintained down to a very coarse image resolution. Artifacts present in CT image data, whether from the physical object or the scanning process, can lead to worse accuracy. These artifacts may affect segmentation threshold choice during geometry reconstruction. In summary, this work is an important first step towards estimating the systematic uncertainty associated with 3-D geometry reconstructions that are utilized as part of image-based modeling applications.

Mention of commercial products does not imply endorsement by NIST.

References:

1. Levine ZH, *J Res Natl Inst Stand Technol*, 2008, Vol 113, 335-340.
2. Standard Reference Material 2087, www.nist.gov/srm.
3. Tan, Y. *et al.* 2011, *Intl. symp. on digital industrial radiology and computed tomography*, Berlin, Germany.

Levine, Zachary; Genc, Karim; Luke, Stephen; Pietiela, Todd; Cotton, Ross; Ache, Benjamin; Young, Phillipe; Horner, Marc; Townsand, Kevin. "Towards Estimating the Uncertainty Associated with 3D Geometry Reconstructions From Medical Image Data."
Paper presented at the 2016 BMES/FDA Frontiers in Medical Devices Conference, College Park, MD, May 25-May 27, 2016.

A “Smart Component” Data Model In PLM

Yunpeng Li and Utpal Roy
Department of Mechanical and Aerospace Engineering
Syracuse University
Syracuse, New York 13244, USA

Seung-Jun Shin and Y. Tina Lee
Systems Integration Division
National Institute of Standards and Technology
Gaithersburg, Maryland 20899, USA

Abstract—**Physical products are becoming smarter because of their increased number of embedded sensors and their real-time information-processing capabilities. Data analytics, particularly predictive analytics, is one of the most important of these capabilities because it uses statistical or machine-learning techniques to determine causal relations between input and output parameters. Many researchers have addressed the challenges in creating and evaluating predictive models. Few, however, have discussed how to employ such models effectively throughout a product’s life cycle.**

In this paper, we address this issue by extending Product Lifecycle Management (PLM) systems to include “Smart Component” data models that incorporate predictive models as “parts” or “services” of products in their master records in PLM. These smart-component data models can be modularized, composed, reused, traced, maintained, and replaced on demand. We describe a prototype system to demonstrate the feasibility of the proposed data models using an open-source PLM platform.

Keywords—Smart product, smart component, predictive analytics, PLM, PMML, CRISP-DM

I. INTRODUCTION

New information and communication technologies - such as sensor networks, predictive analytics, and cloud computing - are enabling the fast growth of connected “smart products”. Embedding computing and networking functionalities into products is becoming technically and economically feasible [1]. Definitions of smart products can be found in [2-5]. These definitions describe several fundamental capabilities of a smart product. A smart product should (1) possess a globally unique identification; (2) be able to retain or store data about itself; (3) continuously monitor its status and environment; (4) react and adapt to environmental and operational conditions; (5) maintain optimal performance; and, (6) actively communicate with the user, environment, and/or other products and systems.

These capabilities provide smart products with a certain degree of intelligence that enables them to perform reasoning based on known knowledge and to learn new knowledge from past experience. The degree of intelligence of smart products depends on how well they handle information, identify and solve problems, and make good decisions [6]. The increasing use of sensors within smart products provides the data needed for intelligence. Data analytics provides the tools and technologies needed to increase the degree of intelligence.

Data analytics is intended to answer the questions of “what has happened” (descriptive analytics), “what could happen” (predictive analytics), and “what should we do” (prescriptive analytics), using statistical and machine learning techniques [7]. Thought of this way, predictive analytics is a key technology to use past and current behaviors to improve decisions for future actions. That technology can be implemented inside the physical product itself or completely outside the physical product using a cloud-based service. Either way, an up-to-date analytics model is a necessary foundation for such a technology.

Creating smart products requires developing physical products and analytics models in a transdisciplinary approach across mechatronics, software, and service domains. A lifecycle approach is also necessary to capture data and information required by all stakeholders, as well as to exchange that data/information among heterogeneous processes, tools, and information systems. As a foundation for both approaches, we will use the concept of Product Lifecycle Management (PLM), which emerged in the 1990’s. PLM includes a shared platform for the creation, management, and dissemination of product-related information across the extended enterprise [8]. It also provides capabilities to access, use, and maintain product definition information, as well as the business processes related to all lifecycle activities.

Successfully using PLM requires collaboration among data analysts, software engineers, design engineers, and business experts. This is a big challenge because it is often difficult to communicate ideas across multiple disciplines and to integrate the digital representation of those ideas among heterogeneous tools and information systems. The usual approach to address both issues involves standards. While many industrial/open standards (e.g., ISO 10303 STEP [9]) in manufacturing domain have been available for decades [10], none of them support all of the interdisciplinary information needed to capture and communicate those ideas.

On the other hand, data-mining related standards or best practices, such as PMML (Predictive Model Markup Language) [11] and CRISP-DM (CRoss-Industry Standard Process for Data Mining) [12], are widely used in the data analytics community. However, they remain largely underutilized by the manufacturing industry today, and are not supported by the current PLM systems. This is a problem. Another problem involves synchronizing the processes for physical-product development and analytics-model development. This is because development of accurate analytics models greatly relies on new data generated as part of the physical-process development. Because there is an inevitable time lag between these development processes, analytics models will always be one step behind the physical world. This means that inevitably, over

Li, Yunpeng; Roy, Utpal; Shin, Seungjun; Lee, Yung-T.
“A 'Smart Component' Data Model in PLM.”
Paper presented at the 2015 IEEE International Conference on Big Data, Santa Clara, CA, Oct 29-Nov 1, 2015.

time, the predictive performances of those analytical models will decay. To minimize the rate of decay, it is necessary to understand when and how these two processes interact with each other throughout the different lifecycle stages. The key to understanding lies in the data and the information needed for such an interaction.

Many recent literatures have addressed issues related to sensor-data acquisition, data processing, analytics-model building and scoring, visualization and user interaction, as well as security and privacy [13]. However, only a few literatures have presented works related to the management of the analytics models and their composition, which is needed to keep track of the changes to physical products as they move through their lifecycle.

One such work is CL$_2$M (Closed-Loop Lifecycle Management) [14], which is an effort to extend PLM for smart products. It incorporates the PEID (Product Embedded Information Device) technology to collect a product's tag and sensor data, plus other necessary "lifecycle-event" data. As a result, CL$_2$M can provide feedback knowledge into the processes that make the product lifecycle. This work focuses primarily on the data management issues of product identification and sensor data. Another such work is reported by Jain et al. (2008) [15]. Specifically, the authors discuss the challenges regarding building, updating, and sharing complex data-mining models across the model lifecycle. However, this work focuses merely on analytics model management without considering their use for a product.

To our knowledge, no work has attempted to merge these two lifecycles. To do this successfully, it is essential, in our opinion, to unify data models for a product's physical components and the associated analytics models. Such unification allows the data models to be modularized and shared consistently across both lifecycles. In this paper, we describe and implement a uniform, PLM modeling environment that integrates the two heterogeneous models - product and analytics - taking into consideration their lifecycle perspectives. As part of this environment, we propose a "Smart Component" data model to enable composition of unit physical components and unit predictive models in order to reuse, trace, maintain, and replace each individual model on demand.

The paper is organized as follows: Section II briefly reviews the standard metadata and lifecycle models for predictive analytics and identifies their roles and limitations; Section III presents the concepts of "Smart Component" data model and the model's lifecycle management; Section IV illustrates a proof-of-concept implementation to the proposed data model on an open source PLM platform, using a manufacturing case study. We discuss our research limitations and lessons learned from the study in Section V.

II. Standard Metadata and Lifecycle Models for Predictive Analytics

A. *Formal Representation of Predictive Models*

A literature review on the standards for predictive models is reported in our earlier publication [16]. There we argued that PMML could be extended for broader usages in manufacturing. Particularly, predictive models could have the same hierarchical characteristics as a physical product. Thus, predictive "part" models could be built for each physical "part" in the product. Furthermore, the PLM methodology could be applied to both model of the "part" and the "part" itself. PMML uses XML (Extensible Markup Language) to formally encapsulate and represent predictive models. It separates the development and deployment processes of a predictive model, and enables interchange of the model among different data analytics tools and environments.

A predictive model conforming to the PMML specification contains several key elements (see Fig. 1) including (1) a **Header** element that contains general information about the predictive model; (2) a **DataDictionary** element that contains schema definitions for all the possible data fields used by the model; (3) **TransformationDictionary** and/or **LocalTransformations** elements that allow users to map data into a more desirable form to be used by the mining model; and (4) One or more model (**Model** or **MiningModel**) elements that define the structure and scoring method of a mining model. Each model consists of a mining schema based on the type of the model it represents, the detailed model structure, target fields and values, and output elements such as measures of accuracy. The current PMML specification, PMML 4.2.1 [11], supports popular predictive models such as classification, regression, clustering, and association rules.

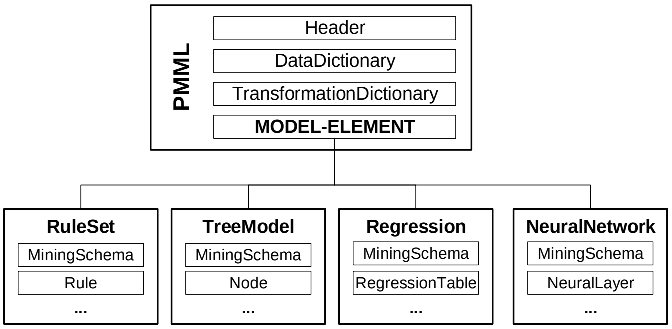


Fig. 1. The PMML model structure [11]

There are three main challenges to get PMML to treat predictive models the same as physical products. First, PMML is primarily designed for representing structures and not data. Data fusion and data management have to rely on external, specific, workflow-based data analytics tools. Second, PMML provides no support for external document references; consequently, there are reductions in the flexibility of exchange, reuse, replacement, versioning, and tracing of the individual models. Third, PMML cannot provide required lifecycle concepts to predictive models; thus it cannot trace the model evolvement from newly available data and algorithms. A formal process model is required to support the lifecycle activities and interactions.

B. *Lifecycle Management of Predictive Models*

An analytics model is the end product of a knowledge discovery and data mining (KDDM) process that uses a formal methodology. That process typically consists of multiple steps executed in sequence, and often includes iterations between steps, which are triggered by a revision process. A literature review on the KDDM process model development can be found in [17][18]. We focus on the CRISP-DM [14] model in this paper because of its industrial origin and adoption. CRISP-DM defines six phases to complete a data analytics project and each phase further defines several key generic tasks and deliverables. The six phases are (see Fig. 2): business understanding, data understanding, data preparation, model building, model evaluation, and model deployment.

Business understanding identifies the project objectives and requirements, and converting them into a data analytics problem definition and a preliminary plan. Data understanding collects initial data, identifies data quality, and explores the data to form initial hypotheses. Data preparation preprocesses the raw data to construct the final dataset. Model building uses various modeling techniques to construct the model and optimize the parameters. Model evaluation thoroughly reviews the steps to create the model, in order to ensure that the model achieves the business objectives. Model deployment organizes and presents the knowledge gained to the stakeholders who use the model.

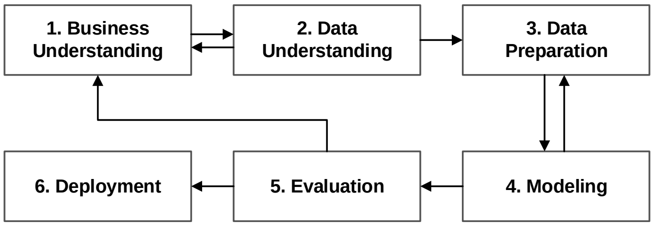


Fig. 2. The CRISP-DM process model [12]

As the leading methodology for data analytics projects [19][20], CRISP-DM has its limitations. First, it does not provide detailed guidelines concerning the iteration processes [17]. Second, it does not standardize the necessary authentications and authorizations in each activity and between activities. Third, it is not closed-loop: there exist no process routines for the model revisions and maintenances after the deployment phase. It becomes even more challenging when considering the synthesis of KDDM process models with other transdisciplinary process models for mechatronics, software, and service [21]. The extension of CRISP-DM or development of new KDDM process models is out of the scope of this paper; instead, we intend to employ this reference model to provide the necessary lifecycle context for predictive model management.

III. Concepts of “Smart Component” Data Model and Lifecycle Management

For brevity, we use the term “physical component” to imply digital representation of a physical product component in this paper. Also, we focus only on predictive analytics models (out of the three data analytics paradigms) without losing the generality of the problem and methodology. At a minimum, a smart product consists of a physical product component (for its form) and an analytics model component (for its “intelligence” implementation). Table I lists a side-by-side comparison between a physical component and a predictive model, revealing that they share commonalities in many aspects, e.g., authoring and management, production planning, visualization, and standards. Both are produced by certain producers and are used by one or more consumers, to fulfill certain designed functions. Individual component/model is produced from certain kinds of raw materials or raw data, and could be supplied by various vendors. The production of the individual consumes resources and it needs deliberate production planning. A master model (the final physical product or analytics model) typically consists of a set of sub models. Each sub model may be composed of several unit models. Thus, the master model can be represented as an assembly tree. Models with common functions can be modularized and standardized for easier reuse, interchange, and composition. A model might be used repeatedly in the same master model or in a different master model and may have variations, thus the model utilization history needs be traced over its lifecycle stages.

This analogy leads to a unified “Smart Component” data model as shown in Fig. 3. Typically, a physical component model consists of metadata definition (e.g., attributes), material definition, structure (i.e., Bill of Materials), alternative components, manufacturer information, relevant documents (e.g., requirement specification and maintenance manual), and neutral electronic files (e.g. ISO 10303 STEP document) for long-term storage and data exchange. Similarly, a complete predictive model also contains these kinds of information. The main idea is that the dataset is treated as the primary “material” to produce a predictive model. A smart component (*SC*) is then composed by one or more physical components (*PCs*) and one or more predictive models (*PMs*), and has configuration rules to reflect their relationships ($REL_{PC,PM}$):

$$SC = < PCs, PMs, REL_{PC,PM} >$$

A predictive model can be treated either as a “part” of a product or as a “service” for the product, depending on its purpose. Once product models and predictive models are modeled in a unified way, they can be composed according to certain configuration rules. Methodologies such as PLM, which are applied typically to only a physical product, now can be applied to a predictive model and then to a smart component. The traditional PLM concept can then be enriched to provide support for smart-products lifecycle management.

In the following sub sections, we detail the lifecycle management concepts that are related to the proposed “Smart Component” data model. It starts with the metadata and relationship management of the datasets and the predictive models. It then deals with the composition of unit predictive models, and the composition of predictive models and physical components. Finally, it provides for the retrieval and consumption of the resulting, composite, smart-component model data. These concepts help build a minimal PLM system that may (1) serve as a data and model repository for the datasets, predictive models, and physical components that build smart products, and (2) be able to respond to any requests from either inside PLM or external applications by providing composed/enriched model information using certain XML-based data formats.

TABLE I. COMPARISON BETWEEN A PHYSICAL COMPONENT AND A PREDICTIVE MODEL

	Physical Component	*Predictive Model*
End Product	An end-product of manufacturing processes	An end-product of computational processes
Development Process	Integrated product design and manufacturing process	A formal knowledge discovery and data mining (KDDM) process
Process Planning	Output: • Manufacturing process selection • Material selection • Operation sequence Resource: • Raw material, work-in-progress stock • Fixture • Machine/tool • Operations (milling, turning, drilling, …)	Output: • Attribute selection • Analytical model selection • Step sequence Resource: • Raw data, intermediate data • Data extract, transform, load (ETL), data pre/post-processing • Algorithms (regression, classification, clustering, association Rules…)
Authoring and Management Tools	• CAD/CAE/CAM • Product Data Management (PDM) • Product Lifecycle Management (PLM)	• Mathematics/Statistics tools • Data Mining packages • Application Lifecycle Management (ALM)
Visualization	2D drawings/3D models	2D/3D plots
Standards/Guidelines	ISO 10303 STEP, IGES, JT, etc.	PMML, PFA, CRISP-DM, etc.

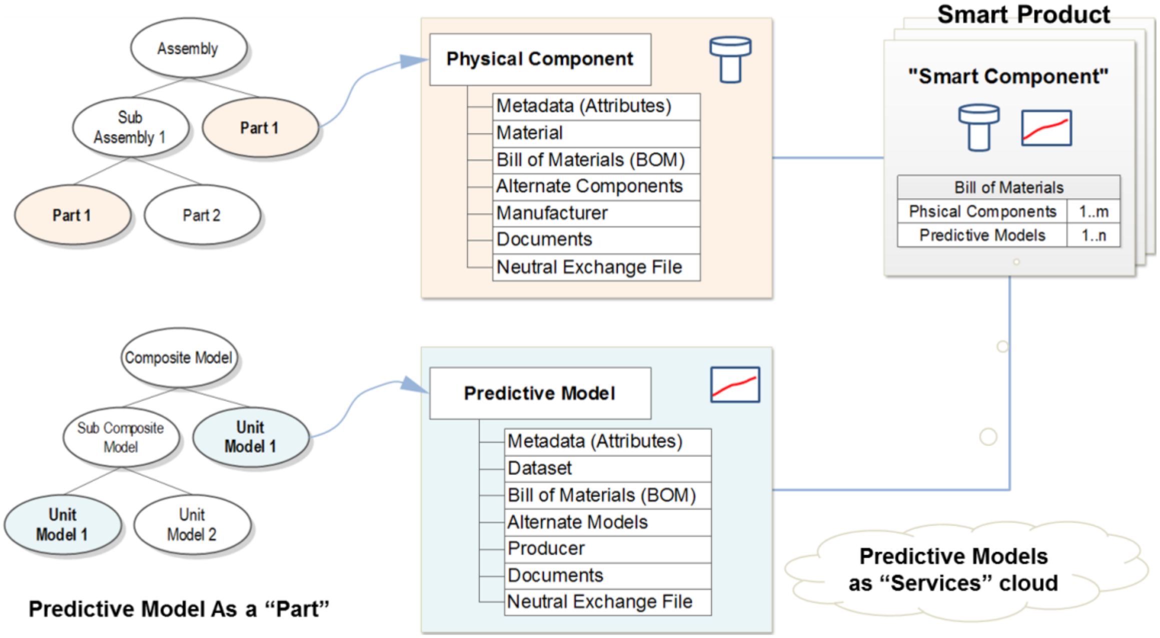


Fig. 3. The "Smart Component" data model

A. *Predictive Model and Dataset Management*

A model is a composite object, containing many other objects, their properties and their relationships [22][23]. In PLM, a product model's structure is described as an assembly tree of parts, in which each part is an object with part properties. Two relationships ("contains" and "where used") are employed to trace the product's structure and every part's usage history. The "Item" is used as a general term for arbitrary artifacts; it provides records for various levels of the bill of materials (BOM) for all products managed in a PLM system.

In the view of predictive models, training and validation datasets are the primary "raw materials" used to create and validate a predictive model. A particular dataset can be used to create or validate many different unit predictive models. As a predictive model evolves over its lifecycle, so will its datasets. Therefore, the management functions must be able to track the changes in the datasets (see Fig. 4). To do this, composition relationships between datasets and predictive models must be established. A more complex predictive model can then be built by composing several unit predictive models. Similarly, a predictive model is used to create a smart component, which is further used to build smart products. This hierarchy of heterogeneous building blocks can be generalized using an Item-Relationship-Item structure, in which each item has its own unique identifier, properties and methods (see Fig. 5). Once such a modular structure is established, all building blocks can be accessed, used, traced and maintained consistently.

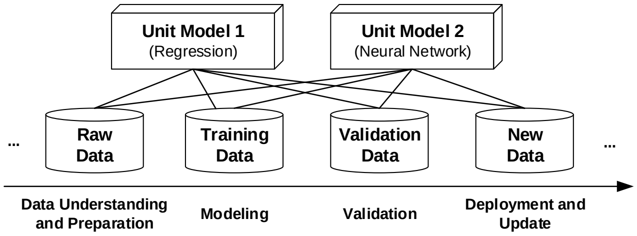


Fig. 4. The relationship of unit predictive models and datasets over the model lifecycle

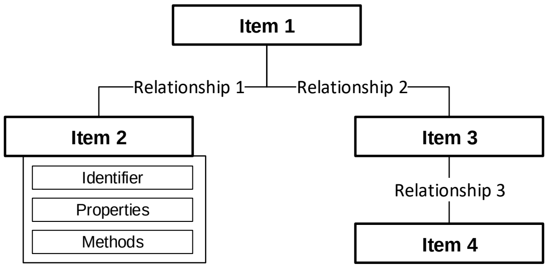


Fig. 5. The generalized Item-Relationship-Item structure in PLM

Creating predictive models in PLM systems requires importing, mapping, and merging the required predictive-model schema (e.g., PMML) with the existing, physical-product schema (e.g., ISO 10303 STEP). Model management [22] is one of the formal methodologies to integrate complex models represented by different schema formats. The **DataDictionary** schema defined in the current PMML specification can be used to formally model the dataset items. As noted, the composition of a predictive model and its relevant datasets is necessary to create and validate the predictive model. The lifecycle stages and deliverables defined in the CRISP-DM reference model can be used to determine when an appropriate dataset should be attached to the predictive model and when the predictive model should be used by a smart component.

B. Composition of Unit Predictive Models

PMML supports model ensembles and model chains. The **Segmentation** element defined in PMML allows users to represent different models for different data segments. This element is also useful to encapsulate multiple models into a single PMML document. However, this also reduces the flexibility of exchange, reuse, replacement, versioning, and tracing of an individual model within the PMML document. The modular design principal for physical products can address this problem.

The elements defined in the PMML specification can be modeled as different items supported by their hierarchical relationships. For instance, the root PMML element has a relationship to a MODEL-ELEMENT element. The MODEL-ELEMENT element can be defined as a “hybrid item” in PLM so that it accepts different predictive models including regression models, neural network models, and ruleset models. Each unit-predictive-model item can then be inserted into a master PMML item or multiple PMML items. This enables a given unit model to be reused as demanded.

In our previous work [16], we illustrated a model to predict manufacturing operations for features of a prismatic part. That model comprised two unit models: a ruleset model and a tree model. The ruleset model is for non-hole features such as a face, a slot, or a pocket; the tree model is for hole features. These two unit models can be combined together to make prediction for different feature categories. This multi-model structure can be modeled simply by inserting the two unit models into the master PMML item.

Configuration rules, which support the selection of a particular model to meet certain conditions, can be created as a separate ruleset model. This model can then be added into the master PMML item and also linked to the involved unit models. In general, a master PMML item can contain all the necessary unit models plus at least one configuration ruleset model (where we assume all configuration rules can be decomposed and represented as IF-THEN rules to form a ruleset model). Fig. 6 illustrates the conceptual structure of this composite predictive model.

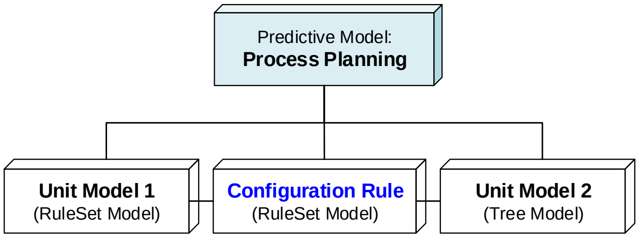


Fig. 6. A predictive model including two heterogeneous unit models

A predictive model can be modeled at different granularity levels. For instance, we can treat the whole predictive model as a single item with the metadata as its properties and then attach a PMML document to the item. This is the traditional approach for document-centric data management. It is the simplest way to maintain the document information without losing any raw information because the original file can be referenced as needed. The primary drawback of this approach is that those sub-elements within the PMML document cannot be accessed individually afterwards.

The other approach is to model the sub-elements of the PMML document as items. This approach increases the modularity and reusability of sub-elements that include data fields, data transformations, and models. For example, two predictive models may use the same data fields but different algorithms; or, two polynomial regression models may have the same model structures with the same mining fields and different predictor coefficients. Modeling sub-elements provides a finer granularity of information for controlling the model structure. This allows users to take full advantage of PLM functions, such as versioning, change management, and configuration management. However, a compromise must be made since there are additional costs for a more granular data management: it means more data needs to be stored and more complicated relationships need to be traced.

C. *Composition of Physical Components and Predictive Models*

As mentioned previously, a predictive model can be treated in two ways: as a "part" or as a "service", depending on the functional role and location of the model. For example, a CNC (Computer Numerical Control) machine can be equipped with an energy-consumption predictive model to estimate its power usage based on the proposed process parameters, which include current feed rate, spindle speed, cutting depth, and cutting diameter. The values for these parameters are collected from the machine's built-in sensors. In this case, the energy consumption predictive model is a "part" of the CNC machine.

On the other hand, when we consider a part produced by this machine, the energy consumption predictive model becomes a "service" for the part because the predictive model functions outside the part (Fig. 7). Both the CNC machine and the part can also use other predictive models as "services", for instance, a process planning model that defines the operation sequence to produce machined parts.

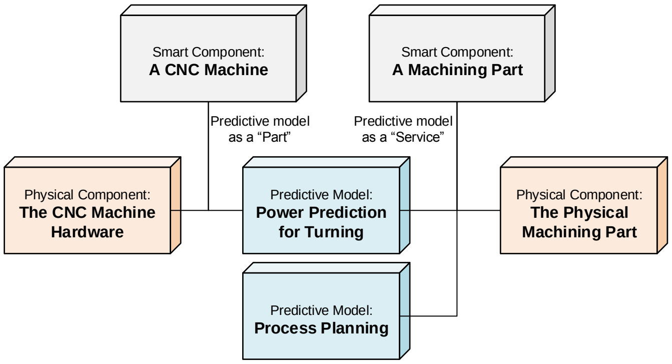


Fig. 7. Predictive model as a "Part" or a "Service"

We need to apply different relationships to connect the physical components to "part" predictive models and to "service" predictive models. The "part" relationship requires a strict composition relationship between the smart component and the predictive model. The "service" relationship is a weaker association relationship and it is optional to a smart component. Similar to the configuration rules for composition of predictive models, the configuration rules for composition of physical-predictive models can also be represented as a ruleset model.

D. *"Smart Component" Model Retrieval*

The PLM system is, essentially, a data repository. As such, it stores all the available instance data and instance models. It also stores all the necessary lifecycle information such as states and revisions of the data and the models. A smart component has metadata for self-description and predictive models as its intelligent parts. Thus, it can predict its own behaviors based on the data collected for the component. A general framework to retrieve and utilize the smart-component model data is illustrated in Fig. 8. The "Smart Component" model can either be (1) executed inside the PLM system using PLM built-in execution engines and methods, or (2) retrieved and utilized from an external application through some web services or application programming interfaces (API).

The data and models in the repository may be exposed directly to external applications (see the dash line between the "Repository" block and the "Application" block). The PLM system should be capable of returning information regarding any physical component model, dataset, unit predictive model, and any of their compositions, corresponding to different levels of queries requested.

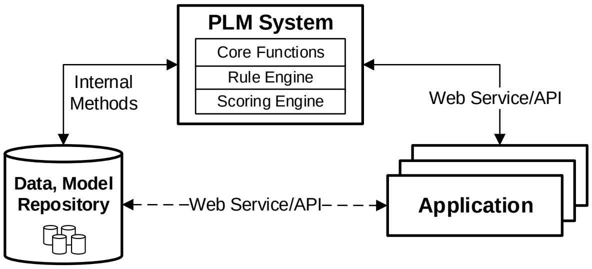


Fig. 8. Smart component model retrieval and consumption

IV. Implementation

In this section, we illustrate a proof-of-concept implementation using a CNC machine equipped with a power prediction module. The power prediction module contains predictive models that are created based on several parameters related to the machining process. The module can be used with real-time process data. We choose the open source PLM platform, Aras Innovator PLM [24], for the implementation. The core PLM functions provided by this platform allow us to focus on implementing the proposed data model and applications.

A. *PLM Platform*

Aras Innovator is an object-oriented, web-based PLM platform as part of a service-oriented architecture (SOA) [25]. Aras Innovator uses the concepts **Item** and **Relationship** to abstract arbitrary objects and connections between objects. Everything in Aras Innovator is an item, which is an instance of an **ItemType**, which itself is an item too. Each item has a 32-character GUID (Globally Unique Identifier). An item may have relationships to other items; a relationship is defined by **RelationshipType**, which is also an item. The relationship type rule is defined by using three properties: the source (parent) item, the related (child) item, and the relationship item. This Item-Relationship-Item architecture is suitable to capture our conceptual model described in Fig. 5.

Aras Innovator uses two workflow models to support lifecycle activities: state-based and activity-based. The state-based workflow model, which is named **Lifecycle Map,** tracks the state of an item during its lifecycle. A lifecycle map consists of a series of states (actions and steps) and transitions (paths between the different states) that an item instance traverses during its existence. The activity-based model, which is named **Workflow Map,** tracks the work that people actually perform. A workflow map consists of activities and paths, in which each activity represents a unit of work that must be performed. An activity contains the task list, the assignment to users responsible for these tasks, notifications, and time spent on the activity. A workflow map can be accessed from the entry of a lifecycle state and in turn the activities within the workflow map can promote the lifecycle to the next states.

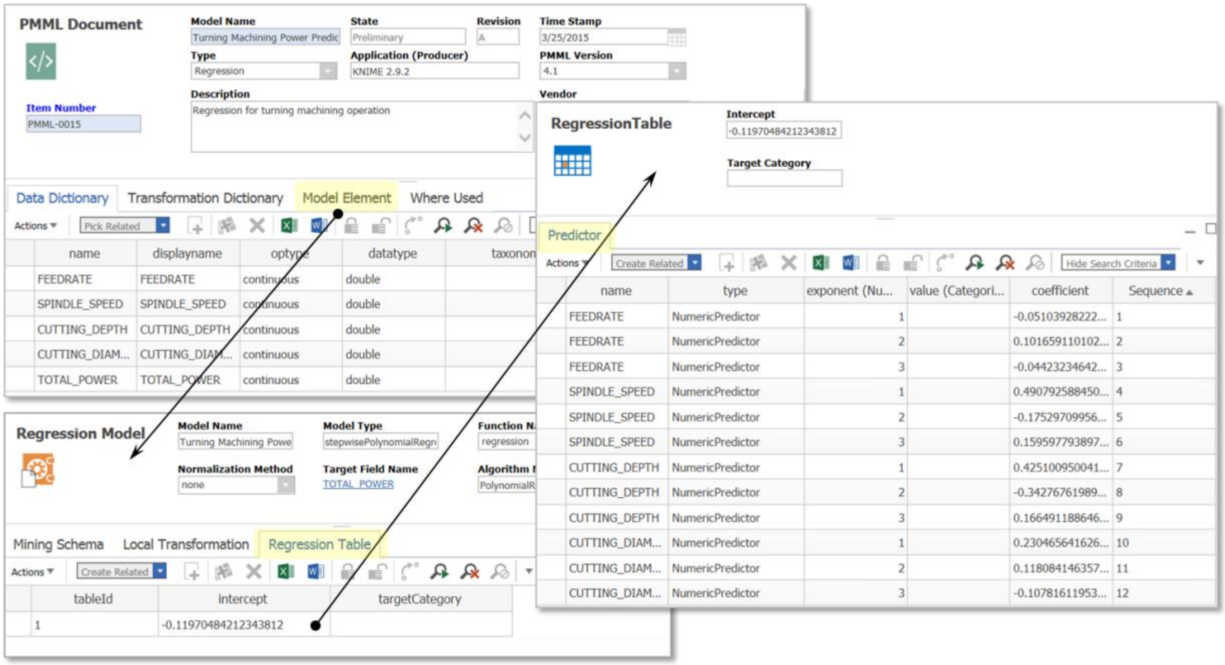
B. *Case Description*

Energy consumption is an important performance indicator. Power consumption is a measured scalar value, which is used to calculate the energy consumption by integrating power with machining time. Therefore, the ability to predicting power consumption enables the energy efficiency of the CNC machines to be monitored and controlled proactively. Let's consider a scenario in which a CNC machine executes roughing operations to produce turned-parts from cylindrical work pieces. It produces a weekly batch of 350 parts made of aluminum and 150 parts made of steel. We use a CNC machine simulator to generate time series data regarding three process parameters: feed rate, spindle speed, and cutting depth [26]. Table II lists the ranges of these process parameters to generate a simulation dataset. This dataset is used to train a cubic polynomial-based regression model as shown in the equation (1).

TABLE II. RANGE OF PROCESS PARAMETERS IN MACHING

Parameter	*Unit*	*Aluminum*	*Steel*
Feed rate	mm/rev	0.1 ~ 0.5	0.2 ~ 0.6
Spindle speed	rad/s	94 ~ 209	94 ~ 126
Cutting depth	mm	1 ~ 4	2 ~ 6

$$\mathbf{TOTAL\_POWER} = \mathrm{B}_{00} + \sum_{k=1}^{3} \mathrm{B}_{1k} \cdot \mathbf{FEEDRATE}^{k} + \sum_{k=1}^{3} \mathrm{B}_{2k} \cdot \mathbf{SPINDLE\_SPEED}^{k} + \sum_{k=1}^{3} \mathrm{B}_{3k} \cdot \mathbf{CUTTING\_DEPTH}^{k} + \sum_{k=1}^{3} \mathrm{B}_{4k} \cdot \mathbf{CUTTING\_DIAMETER}^{k} \qquad (1)$$



PMML Document

Item Number: PMML-0015

Model Name: Turning Machining Power Predic

State: Preliminary

Revision: A

Time Stamp: 3/25/2015

Type: Regression

Application (Producer): KNIME 2.9.2

PMML Version: 4.1

Description: Regression for turning machining operation

Vendor:

name	displayname	optype	datatype	taxonon
FEEDRATE	FEEDRATE	continuous	double	
SPINDLE_SPEED	SPINDLE_SPEED	continuous	double	
CUTTING_DEPTH	CUTTING_DEPTH	continuous	double	
CUTTING_DIAM...	CUTTING_DIAM...	continuous	double	
TOTAL_POWER	TOTAL_POWER	continuous	double	

Regression Model

Model Name: Turning Machining Powe

Model Type: stepwisePolynomialRegr

Function N.: regression

Normalization Method: none

Target Field Name: TOTAL_POWER

Algorithm N: PolynomialR

tableId	intercept	targetCategory
1	-0.11970484212343812	

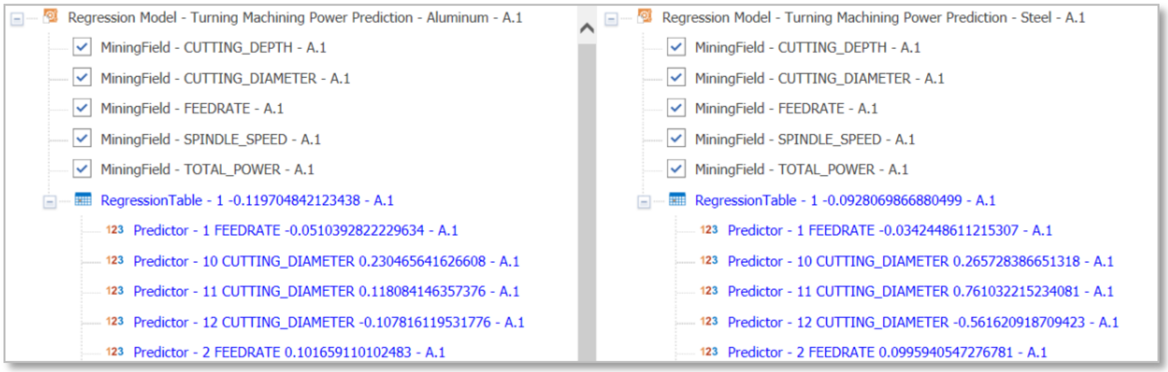
RegressionTable

Intercept: -0.11970484212343812

Target Category:

name	type	exponent (Nu...	value (Categori...	coefficient	Sequence ▲
FEEDRATE	NumericPredictor	1		-0.05103928222...	1
FEEDRATE	NumericPredictor	2		0.101659110102...	2
FEEDRATE	NumericPredictor	3		-0.04423234642...	3
SPINDLE_SPEED	NumericPredictor	1		0.490792588450...	4
SPINDLE_SPEED	NumericPredictor	2		-0.17529709956...	5
SPINDLE_SPEED	NumericPredictor	3		0.159597793897...	6
CUTTING_DEPTH	NumericPredictor	1		0.425100950041...	7
CUTTING_DEPTH	NumericPredictor	2		-0.34276761989...	8
CUTTING_DEPTH	NumericPredictor	3		0.166491188646...	9
CUTTING_DIAM...	NumericPredictor	1		0.230465641626...	10
CUTTING_DIAM...	NumericPredictor	2		0.118084146357...	11
CUTTING_DIAM...	NumericPredictor	3		-0.10781611953...	12

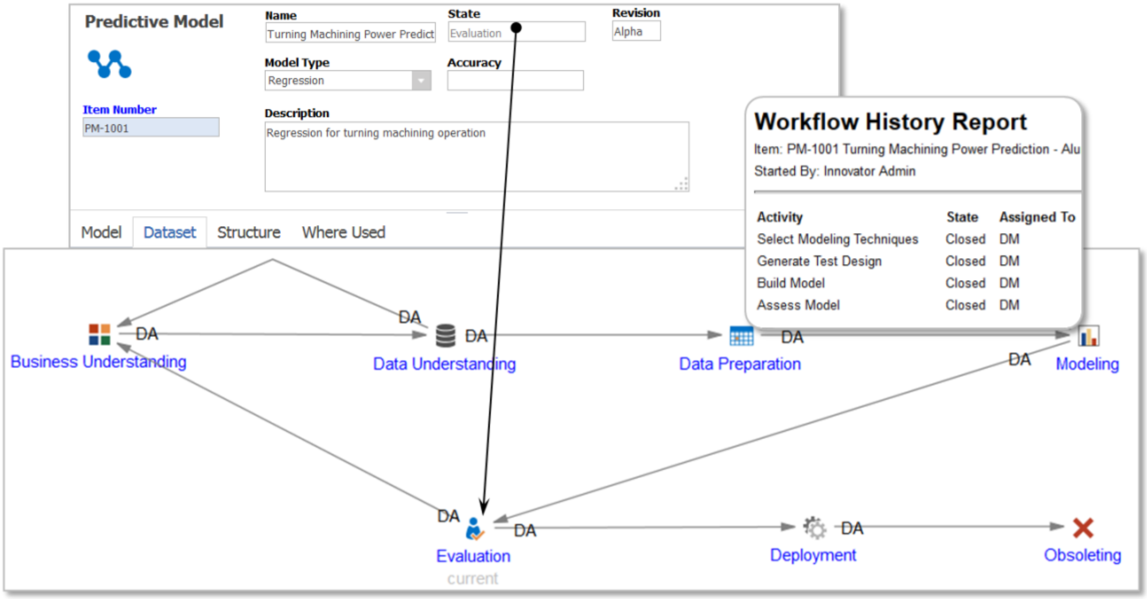
Fig. 9. A PMML regression model's metadata modeled in the PLM system



Regression Model - Turning Machining Power Prediction - Aluminum - A.1
- ☑ MiningField - CUTTING_DEPTH - A.1
- ☑ MiningField - CUTTING_DIAMETER - A.1
- ☑ MiningField - FEEDRATE - A.1
- ☑ MiningField - SPINDLE_SPEED - A.1
- ☑ MiningField - TOTAL_POWER - A.1
- RegressionTable - 1 -0.119704842123438 - A.1
  - 123 Predictor - 1 FEEDRATE -0.0510392822229634 - A.1
  - 123 Predictor - 10 CUTTING_DIAMETER 0.230465641626608 - A.1
  - 123 Predictor - 11 CUTTING_DIAMETER 0.118084146357376 - A.1
  - 123 Predictor - 12 CUTTING_DIAMETER -0.107816119531776 - A.1
  - 123 Predictor - 2 FEEDRATE 0.101659110102483 - A.1

Regression Model - Turning Machining Power Prediction - Steel - A.1
- ☑ MiningField - CUTTING_DEPTH - A.1
- ☑ MiningField - CUTTING_DIAMETER - A.1
- ☑ MiningField - FEEDRATE - A.1
- ☑ MiningField - SPINDLE_SPEED - A.1
- ☑ MiningField - TOTAL_POWER - A.1
- RegressionTable - 1 -0.0928069866880499 - A.1
  - 123 Predictor - 1 FEEDRATE -0.0342448611215307 - A.1
  - 123 Predictor - 10 CUTTING_DIAMETER 0.265728386651318 - A.1
  - 123 Predictor - 11 CUTTING_DIAMETER 0.761032215234081 - A.1
  - 123 Predictor - 12 CUTTING_DIAMETER -0.561620918709423 - A.1
  - 123 Predictor - 2 FEEDRATE 0.0995940547276781 - A.1

Fig. 10. The comparison between the structures of two regression models (one is for Aluminum material and the other is for Steel material)



Predictive Model

Item Number: PM-1001

Name: Turning Machining Power Predict

State: Evaluation

Revision: Alpha

Model Type: Regression

Accuracy:

Description: Regression for turning machining operation

Model | Dataset | Structure | Where Used

Workflow History Report

Item: PM-1001 Turning Machining Power Prediction - Alu

Started By: Innovator Admin

Activity	State	Assigned To
Select Modeling Techniques	Closed	DM
Generate Test Design	Closed	DM
Build Model	Closed	DM
Assess Model	Closed	DM

Fig. 11. The lifecycle map of a predictive model

The regression model uses four machining process parameters as predictors: feed rate, spindle speed, cutting depth, and cutting diameter. Here, the cutting diameter is the outermost dimension of the work piece being turned and can be calculated from the cutting depth. It is added to the model due to its influence on the cutting power [26]. The process parameters vary for producing parts made of two different materials. Thus, the resultant two unit regression models have the exact same structures but different intercepts (B_{00}) and coefficients (B_{11}-B_{43}) for individual predictors of their regression equations. The two unit regression models can be then individually used. They can also be composed into a single power prediction model, using material as a parameter to create the model configuration rule. Then, the power prediction model is used as a "part" by any compatible CNC machine product and predicts the machine's behavior regarding energy consumption.

C. *Predictive Model Metadata and Lifecycle Management*

The hierarchy of the PMML elements shown in Fig. 1 can be mapped easily to the Item-Relationship-Item structure of the PLM system. For example, the root **PMML** element and the **DataField** element can be modeled as two item types and can be connected with a **DataDictionary** relationship. Similarly the **MiningSchema** is modeled as a relationship to connect the root **MODEL-ELEMENT** with the **MiningField** element.

Fig. 9 shows the implementation of the regression model for aluminum materials and its master PMML item to invoke the model. The PMML's elements are now organized conforming to the Item-Relationship-Item structure - each element's metadata has been collected and presented in a client form intuitively. This example PMML document has five data fields and one regression model. The regression model contains one regression table that consists of descriptive information of each predictor. Fig. 10 demonstrates that the mining fields are reused in the two unit polynomial regression models with the same model structures but different coefficients for each predictor.

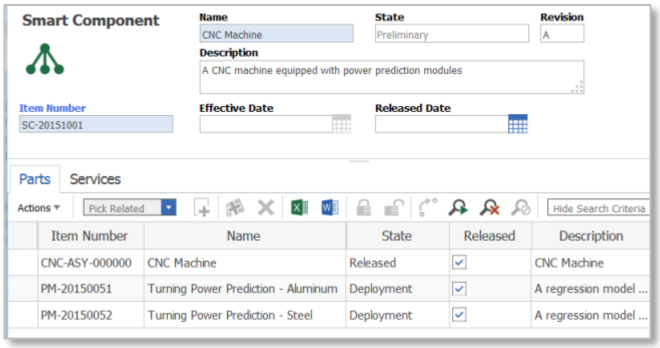
The phases and generic tasks defined in the CRISP-DM model can be implemented in the PLM system as one lifecycle map and several workflow maps. Detailed tasks and deliverables of each phase can also be modeled. Fig. 11 shows a predictive model that has completed the "Modeling" phase, and is currently in the "Evaluation" phase of its lifecycle. Its version is labeled as "Alpha", since it has been neither released nor deployed yet. The workflow model enables different participants to interact with one another following certain business rules. For illustration purpose, we assume the model development process involves two user groups "DA" and "DM", which stands for "Data Analytics" and "Data Mining" respectively, who have different roles in different lifecycle stages. A user in the DM group focuses on the activities and tasks during the "Modeling" phase. He/she (1) requires the preprocessing work to be completed by other users in the DA group, and (2) submits the completed predictive model to appropriate users in the DA group for further post-processing.

The lifecycle model in the PLM system can also capture the appropriate relationships between the predictive model and its relevant datasets. For instance, the training dataset can only be used in the "Modeling" phase, and a newer training dataset may be used to update the predictive model during a model- revision process.

D. *Smart Component Model Composition and Consumption*

A smart component's master model can contain one or more physical components and one or more predictive models. For the CNC machine case, we treat the two regression models as two different predictive models and as two "parts" of the machine (see Fig. 12). There are different ways to categorize these predictive models: either in the power subsystem of the machine, or in the control subsystem of the machine - the choice depends on how the manufacturer built the machine. Furthermore, the power prediction model can be easily reused by different CNC machines. It can also be updated or replaced when new data or more effective algorithms are available. These updates can be recorded and traced afterwards.

Also, as mentioned in Section III C, this CNC machine can be equipped with a process planning model as a service module. In this case, the process planning model will be aware of the CNC machine as a resource and will take consideration of it with other constraints when any process planning process is initiated.



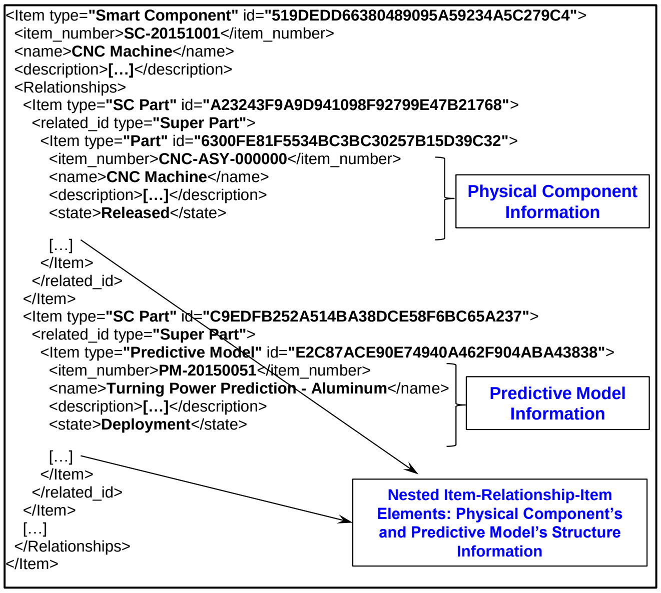
Smart Component

Name: CNC Machine
State: Preliminary
Revision: A
Description: A CNC machine equipped with power prediction modules
Item Number: SC-20151001
Effective Date:
Released Date:

Item Number	Name	State	Released	Description
CNC-ASY-000000	CNC Machine	Released	☑	CNC Machine
PM-20150051	Turning Power Prediction - Aluminum	Deployment	☑	A regression model ...
PM-20150052	Turning Power Prediction - Steel	Deployment	☑	A regression model ...

Fig. 12. The smart component implementation for a CNC machine

The composite smart-component model can then be retrieved at any level from inside PLM and/or from outside applications. Fig. 13 shows a skeleton XML data from the PLM system that responds to a model query. The response to the query includes (1) all the necessary model data such as physical components, predictive models and their relevant datasets, and (2) all lifecycle information such as lifecycle stages and revisions. These data can be further parsed by the rule engine and the scoring engine embedded inside the PLM system or used in an external application (for an example of an external application, see [26]).



```
<Item type="Smart Component" id="519DEDD66380489095A59234A5C279C4">
 <item_number>SC-20151001</item_number>
 <name>CNC Machine</name>
 <description>[…]</description>
 <Relationships>
  <Item type="SC Part" id="A23243F9A9D941098F92799E47B21768">
   <related_id type="Super Part">
    <Item type="Part" id="6300FE81F5534BC3BC30257B15D39C32">
     <item_number>CNC-ASY-000000</item_number>
     <name>CNC Machine</name>
     <description>[…]</description>
     <state>Released</state>

     […]
    </Item>
   </related_id>
  </Item>
  <Item type="SC Part" id="C9EDFB252A514BA38DCE58F6BC65A237">
   <related_id type="Super Part">
    <Item type="Predictive Model" id="E2C87ACE90E74940A462F904ABA43838">
     <item_number>PM-20150051</item_number>
     <name>Turning Power Prediction - Aluminum</name>
     <description>[…]</description>
     <state>Deployment</state>

     […]
    </Item>
   </related_id>
  </Item>
  […]
 </Relationships>
</Item>
```

Physical Component Information
Predictive Model Information
Nested Item-Relationship-Item Elements: Physical Component's and Predictive Model's Structure Information

Fig. 13. The XML-based response from the PLM system

V. Lesson Learned and Discussion

Based on the observed commonalities between physical components and predictive models, we proposed a "Smart Component" data model to consistently compose both. The composition allows a predictive model taking advantage of the PLM capability that is traditionally designed for physical product development. The intelligence embedded in the predictive models, allows the proposed "Smart Component" to provide important insights to both design and process planning. The data model enables engineers, data analysts, and other stakeholders to collaborate on a common platform to develop smart products. It also serves as the basic foundation for building smart devices, smart equipment, and smart services, which are the key components of a smart manufacturing system.

The PMML specification and the CRISP-DM process model are widely adopted by industrial practitioners, by open source toolkits, and by commercial software for data analytics projects. We integrate them in an open source PLM platform for representing our smart component's schema and instances at different stages of its lifecycle. This integration has further enhanced the PLM's overall capability for predictive-model lifecycle management. By providing capability for composition of datasets and heterogeneous predictive models in PLM, we demonstrate how (1) to overcome the limitations of the present PMML standard that does not support the data representation, and (2) to reuse a unit model that has been encapsulated into a single PMML document with other unit models. The proposed technique in implementing the predictive model in PLM could provide a reference for future extension or enhancement of the current PMML specification. The lifecycle and workflow models available in the PLM system are leveraged to track and trace both unit and composite models in various use case scenarios. This makes it easier to update, replace, and maintain unit predictive models.

However, there remain important issues which need further attention. First, not all predictive models, specifically newly developed algorithms, are covered by the current PMML specification. The approach to incorporate new predictive models would be similar to the current approach, provided the new models can also be formally represented as an Item-Relationship-Item structure. Second, the required information granularity for implementing PMML elements in the PLM system, at different levels of abstraction, should be standardized, if possible, to avoid the unnecessarily high costs of data storage and data entry. Third, the current CRISP-DM reference model is complicated, and is also incomplete. It cannot be fully implemented in a PLM system without substantial efforts. The general authentications and authorizations of each activity as well as conditions to trigger/terminate iterations are not yet clearly defined. Processes for model revision and maintenance are not included in the current CRISP-DM specification. Another challenge is to determine the best practice of modeling the configuration rules for composition of models. We treat the configuration rules as a ruleset predictive model in this paper; however, this assumption requires validation with broader applications. These issues will be addressed in our future studies.

Acknowledgments

This work has been sponsored under the cooperative agreement 70NANB12H274 between the National Institute of Standards and Technology (NIST) and Syracuse University.

Disclaimers

No approval or endorsement of any commercial products by the National Institute of Standards and Technology (NIST) is intended or implied. Certain company names are identified in the paper to facilitate understanding. Such identification does not imply that their products are necessarily the best available for the purpose. The work described herein was funded by the United States Government and is not subject to copyright.

References

[1] The Economist Intelligent Unit (EIU). (2015) Developing smart products. Survey Report. [online] http://www.economistinsights.com/technology-innovation/analysis/developing-smart-products (Accessed September 15, 2015)

[2] Mühlhäuser, M. (2008) 'Smart Products: An Introduction', Constructing Ambient Intelligence, Vol. 11, pp. 158-164.

[3] McFarlane, D., Sarma, S., Chirn, J.L., Wong, C.Y. and Ashton, K. (2003) 'Auto ID systems and intelligent manufacturing control', Engineering Applications of Artificial Intelligence, Vol. 16, No. 4, pp. 365-376.

[4] Kärkkäinen, M., Holmström, J., Främling, K. and Artto, K. (2003) 'Intelligent products – a step towards a more effective project delivery chain', Computers in Industry, Vol. 50, No. 2, pp. 141-151.

[5] Ventä, O. (2007) Intelligent products and systems. Technical report, VTT.

[6] Meyer, G.G., Främling, K. and Holmström, J. (2008) 'Intelligent Products: A survey", Computers in Industry, Vol. 60, No. 3, pp. 137-148.

[7] IBM Software. (2013) Descriptive, predictive, prescriptive: Transforming asset and facilities management with analytics. White Paper. (TIW14162USEN)

[8] Ameri, F. and Dutta, D. (2005) 'Product Lifecycle Management: Closing the Knowledge Loops', Computer-Aided Design and Applications, Vol. 2, No. 5, pp. 577-590.

[9] International Organization for Standardization (2014) ISO 10303-242:2014: Industrial automation systems and integration -- Product data representation and exchange -- Part 242: Application protocol: Managed model-based 3D engeineering. Geneva, ISO.

[10] Gifford, C., delaHostria, E., Noller, D., Childress, L. and Boyd, A. (2006) Related Manufacturing Integration Standards, A Survey. MESA International, ISA, GE Fanuc Automation, Rockwell Automation, and IBM Corporation.

[11] Data Mining Group. [online] http://www.dmg.org/ (Accessed September 15, 2015)

[12] Shearer, C. (2000) 'The CRISP-DM Model: The New Blueprint for Data Mining', Journal of Data Warehousing, Vol. 5, No. 4, pp. 13-22.

[13] Assuncao, M.D., Calheiros, R.N., Bianchi, S., Netto, M.A.S. and Buyya, R. (2015) 'Big Data computing and clouds: Trends and future directions', Journal of Parallel and Distributed Computing, Vol. 79-80, pp. 3-15.

[14] Kiritsis, D. (2011) 'Closed-loop PLM for intelligent products in the era of the Internet of things', Computer-Aided Design, Vol.43, No. 5, pp. 479-501.

[15] Jain, J., Ari, I. and Li, J. (2008) 'Understanding the challenges faced during the management of data mining models', in the Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology, New York, NY, USA.

[16] Li, Y., Roy, U., Lee, Y.T. and Rachuri, S. (2015) 'Integrating Rule-based Systems and Data Analytics Tools Using Open Standard PMML', in ASME IDETC/CIE 2015: the Proceedings of ASME 2015 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference, Boston, Massachusetts, USA.

[17] Kurgan, L.A. and Musilek, P. (2006) 'A survey of Knowledge Discovery and Data Mining process models', The Knowledge Engineering Review, Vol. 21, No. 1, pp. 1-24.

[18] Marban, O., Mariscal, G. and Segovia, J. (2009) 'A Data Mining & Knowledge Discovery Process Model', in Ponce, J. and Karahoca, A. (Eds.), Data Mining and Knowledge Discovery in Real Life Applications, InTech, Vienna, Austria.

[19] KDnuggets. (2014) CRISP-DM, still the top methodology for analytics, data mining, or data science projects. [online] http://www.kdnuggets.com/2014/10/crisp-dm-top-methodology-analytics-data-mining-data-science-projects.html (Accessed September 15, 2015)

[20] Oracle. (2013) Information Management and Big Data: A Reference Architecture. White Paper.

[21] Gericke, K. and Blessing, L. (2012) 'An Analysis of Design Process Models across Disciplines', in the Processings of the 12th International Design Conference, Dubrovnik, Croatia, pp. 171-180.

[22] Bernstein, P.A., Halevy, A.Y. and Pottinger, R.A. (2000) 'A vision for management of complex models', ACM SIGMOD Record, Vol. 29, No. 4, pp. 55-63.

[23] Bernstein, P.A. (2003) 'Applying Model Management to Classical Meta Data Problems', in the Proceedings of the 2003 CIDR Conference, pp. 209-220.

[24] Aras Product Lifecycle Management. [online] http://www.aras.com/ (Accessed September 15, 2015)

[25] CIMdata (2014) Aras Innovator: Redefining Customization & Upgrades. CIMdata Commentary.

[26] Shin, S., Woo, J., Kim, D., Kumaraguru, S. and Rachuri, S. (2015) 'Developing a virtual machining model to generate MTConnect machine-monitoring data from STEP-NC', International Journal of Production Research.

[online] http://dx.doi.org/10.1080/00207543.2015.1064182 (Accessed September 15, 2015)

Extinguishment and Enhancement of Propane Cup-Burner Flames by Halon and Alternative Agents

Takahashi, F.[1]*, Katta, V. R.[2], Linteris, G. T.[3], and Babushok, V. I.[3]

[1]Case Western Reserve University, Department of Mechanical & Aerospace Engineering, Cleveland, Ohio, USA.
[2]Innovative Scientific Solutions, Inc., Dayton, Ohio, USA.
[3]National Institute of Standards and Technology, Gaithersburg, Maryland, USA.
**Corresponding author email: fxt13@case.edu*

ABSTRACT

Computations of cup-burner flames in normal gravity have been performed using propane as the fuel, in addition to a propane-ethanol-water mixture studied previously, to reveal the combustion inhibition and enhancement by the CF_3Br (halon 1301) and potential alternative fire-extinguishing agents (C_2HF_5, $C_2HF_3Cl_2$, and $C_3H_2F_3Br$). The time-dependent, two-dimensional numerical code, which includes a detailed kinetic model (up to 241 species and 3918 reactions), diffusive transport, and a gray-gas radiation model, reveals a unique *two-zone* flame structure. For propane, general trends in the structure are similar to those of the fuel mixture. The peak reactivity spot (i.e., reaction kernel) at the flame base stabilizes a trailing flame, which is inclined inwardly by a buoyancy-induced entrainment flow. As the volume fraction of agent in the coflow increases gradually, the *premixed*-like reaction kernel weakens, thus inducing the flame base detachment from the burner rim and blowoff-type extinguishment eventually. The H_2O in the inner zone is converted further, primarily in the outer zone, to HF and CF_2O through exothermic reactions most significantly with the C_2HF_5 addition. Despite endothermic decomposition of the agent, exothermic reactions of the inhibitor fragments also contribute to the heat-release rate in the outer zone. Although the rates of formation (and associated heat-release rates) of HF and CF_2O are lower for propane, compared to the fuel mixture, two heat-release-rate peaks in the *two-zone* flame structure in the trailing flame are comparable for both fuels. A main heat-release step to form CO_2 in the hydrocarbon-O_2 combustion takes place in-between the two zones. The total heat release of the entire flame decreases (inhibiting) for CF_3Br but increases (enhancing) for the halon alternative agents, particularly C_2HF_5 and $C_2HF_3Cl_2$. Addition of C_2HF_5 resultes in unusual (non-chain branching) reactions and increases total heat release (combustion enhancement) primarily in the trailing *diffusion* flame.

KEYWORDS: Aircraft cargo-bay fire suppression, Diffusion flame stabilization, Halon 1301 replacement, Reaction kernel.

INTRODUCTION

In accordance with the Montreal Protocol to protect the stratospheric ozone layer, the use of the effective fire suppressant CF_3Br (bromotrifluromethane, Halon 1301) has been discontinued except for certain critical applications such as the suppression of cargo-bay fires in aircraft. Halon alternative agents must pass a mandated Federal Aviation Administration (FAA) test [1, 2], in which a simulated explosion of an aerosol can, caused by a fire, must be suppressed by the agent. Unlike CF_3Br, some replacement agents, including C_2HF_5 (pentafluoroethane, HFC-125) and $C_3H_2F_3Br$ (2-bromo-3,3,3-trifluoropropene, 2-BTP), when added at any concentration less than that required for inerting, created a higher over-pressure in the test chamber and thus failed the test.

Recent work [3-5] employing thermodynamic equilibrium and perfectly stirred-reactor calculations (for premixed systems) revealed that higher overpressures in the FAA aerosol can

Proc. of the Eighth International Seminar on Fire & Explosion Hazards (ISFEH8), pp. xx-xx
Edited by J. Chao, V. Molkov, P. Sunderland, F. Tamanini and J. Torero
Published by USTC Press
ISBN: xxx-xxx-xx-xxxx-x :: doi: xx.xxxx/xxx-xxx-xx-xxxx-x_0x-0x

tests might be due to higher heat release from reaction of the inhibitor itself. Nonetheless, the agents should still reduce the overall reaction rate and inhibit the reaction. For diffusion flames, however, the flame structure, combustion inhibition, and enhancement processes are not yet fully understood. In previous papers [6, 7], the authors reported the results of comprehensive numerical simulations for zero- and normal Earth-gravity cup-burner flames using the FAA aerosol can test [ACT] fuel mixture with CF_3Br, C_2HF_5, $C_2HF_3Cl_2$ (2,2-dichloro-1,1,1-trifluoroethane, HCFC-123), and $C_3H_2F_3Br$ added to the coflowing air. Additional numbers of carbon and fluorine atoms in the halon-replacement-agent molecules, compared to CF_3Br, represent potential energy contributions at a fixed concentration if they burn to COF_2 and HF. Nonetheless, the ACT fuel is somewhat unusual in that it contains a large portion of water (which is an important reactant with the halogenated species). The objectives of this study are to investigate the effects of fire-extinguishing agents (with different numbers of carbon and types of halogen) on the diffusion flame and to determine if the enhanced heat release found for the previous simulations with the ACT fuel occur with a more typical hydrocarbon fuel (propane).

COMPUTATIONAL METHOD

A time-dependent, axisymmetric numerical code (UNICORN) [18, 19] is used for the simulation of coflow diffusion flames stabilized on the cup burner. The code solves the axial and radial (z and r) full Navier-Stokes momentum equations, continuity equation, and enthalpy- and species-conservation equations on a staggered-grid system. A clustered mesh system is employed to trace the gradients in flow variables near the flame surface. The thermo-physical properties such as enthalpy, viscosity, thermal conductivity, and binary molecular diffusion of all of the species are calculated from the polynomial curve fits developed for the temperature range 300 K to 5000 K. Mixture viscosity and thermal conductivity are then estimated using the Wilke and Kee expressions, respectively. Molecular diffusion is assumed to be of the binary-diffusion type, and the diffusion velocity of a species is calculated using Fick's law and the effective-diffusion coefficient of that species in the mixture. A simple radiation model [20] based on the optically thin-media and gray-gas assumptions was incorporated into the energy equation. Radiation from CH_4, CO, CO_2, H_2O, HF, COF_2 and soot was considered in the present study. The Plank-mean absorption coefficients are obtained from the literature for the first four species [20] and HF [21]; or calculated for COF_2 [21] and soot [22]. The finite-difference forms of the momentum equations are obtained using an implicit QUICKEST scheme [18], and those of the species and energy equations are obtained using a hybrid scheme of upwind and central differencing.

A comprehensive reaction mechanism was assembled for the simulation of propane or ACT fuel flames with CF_3Br, C_2HF_5, $C_2HF_3Cl_2$, or $C_3H_2F_3Br$ added to air from four mechanisms: the four-carbon hydrocarbon mechanism of Wang and co-workers [23, 24] (111 species and 1566 one-way elementary reactions), detailed reactions of ethanol (5 species and 72 reactions) of Dryer and co-workers [25-27], the bromine and chlorine parts of the mechanism of Babushok et al. [28-31] (10 additional species and 148 reactions), and a subset (51 species and 1200 reactions) of the National Institute of Standards and Technology (NIST) HFC starting mechanism [32, 33]. The final chemical kinetics model (187 species, 3198 reactions for CF_3Br, C_2HF_5, and $C_3H_2F_3Br$; or 241 species and 3918 reactions for $C_2HF_3Cl_2$) and a soot model [22] are integrated into the UNICORN code. Transport data for 139 species are available in the literature; for the remaining 38 species, data are constructed by matching these species with the nearest species (based on molecular weight) with known transport data.

The ACT fuel is a propane-ethanol-water mixture [1, 2] with the volume fractions of the components: $X_{C3H8} = 0.159$, $X_{C2H5OH} = 0.454$, and $X_{H2O} = 0.387$. Table 1 shows the minimum extinguishing concentrations (MECs) of fire-extinguishing agents for n-heptane and propane fuels using the cup-burner method [8, 9] in the literature [8-16]. The calculated MEC obtained in this study are also listed and discussed in the results section.

Table 1. Measured and calculated minimum extinguishing concentrations.

Agent	Chemical	Formula	Measured n-Heptane MEC (%)	Measured Propane MEC (%)	Calculated ACT Fuel MEC (%)	Calculated Propane MEC (%)
Halon 1301	Bromotrifluromethane	CF_3Br	3.0 to 3.2 [10-12]	3.8 to 4.3 [11,13,14]	2.26	2.64
HFC-125	Pentafluoroethane	C_2HF_5	8.7 to 9.3 [8-12]	10.2 to10.4 [11,13]	8.40	7.65
HCFC-123	2,2-dichloro-1,1,1-Trifluoroethane	$C_2HF_3Cl_2$	7.1 to7.4 [15]	N/A	(4.90[b])	(4.60[b])
2-BTP	2-bromo-3,3,3-Trifluoropropene	$C_3H_2F_3Br$	2.6 [16] 4.7 [17][a]	N/A	(1.87[b])	(2.50[b])

[a] The fuel temperature: 50 °C.

[b] A concentration above which the calculation was unable to obtain the solution.

The boundary conditions are treated in the same way as reported in earlier papers [6, 7]. The computational domain is bounded by the axis of symmetry, a chimney wall, and the inflow and outflow boundaries. The burner outer diameter is 28 mm and the chimney inner diameter is 95 mm. The burner wall (4-mm long and 1-mm thick tube) temperature is set at 600 K and the wall surface is under the no-slip velocity condition. The mean fuel velocities for the ACT fuel and propane are 0.853 cm/s and 0.307 cm/s, respectively, and the mean velocity of the oxidizer ("air" [21 % O_2 in nitrogen] with added agent) is 10.7 cm/s at 294 K.

Validation of the code with the kinetic model was performed through the simulation of opposing-jet diffusion flames. The predicted extinction strain rates for propane-air flames (no agent) were within 7.5% of the measured values (with an error margin of 9 %) by Zegers et al. [34]. The predicted extinction agent concentrations for CF_3Br and C_2HF_5 are within 4 % of the measured concentrations in weakly stretched flames and within 25 % in highly stretched flames. Although cup-burner data using the ACT fuel are unavailable for a direct comparison, computation with the assembled reaction mechanism should provide insights into the detailed flame structure.

RESULTS AND DISCUSSION

The flame base supports a trailing flame and controls the flame attachment, detachment, and oscillation processes [35, 36]. Small variations in the agent volume fraction in the coflowing oxidizing stream (X_a) results in profound changes near the extinguishment limit. Figure 1 shows the calculated structure of near-limit propane flames in air with added agent: (a) CF_3Br, X_a=0.0258; (b) C_2HF_5, X_a=0.0765; (c) $C_2HF_3Cl_2$, X_a=0.0455; and (d) $C_3H_2F_3Br$, X_a=0.0246. The variables include the velocity vectors (**v**), isotherms (T), and heat-release rate ($\dot{q}$). The base of the agent-added flames are detached and drift inward a few mm away from the burner rim by the nearly horizontal entrainment flow. In contrast to zero-gravity ($0g_n$) flames [6], which are formed vertically, the normal gravity ($1g_n$) flame inclines inwardly due to the streamline shrinkage in the accelerating buoyancy-induced flow. The contours of the heat-release rate show a peak reactivity spot (i.e., the *reaction kernel* [35]) at a height from the burner rim, z_k = 0.8 mm to 1.8 mm. The chain radical species (H, O, and OH) as well as heat diffuse back against the oxygen-rich flow at the flame base (edge), thus promoting vigorous reactions to form the reaction kernel.

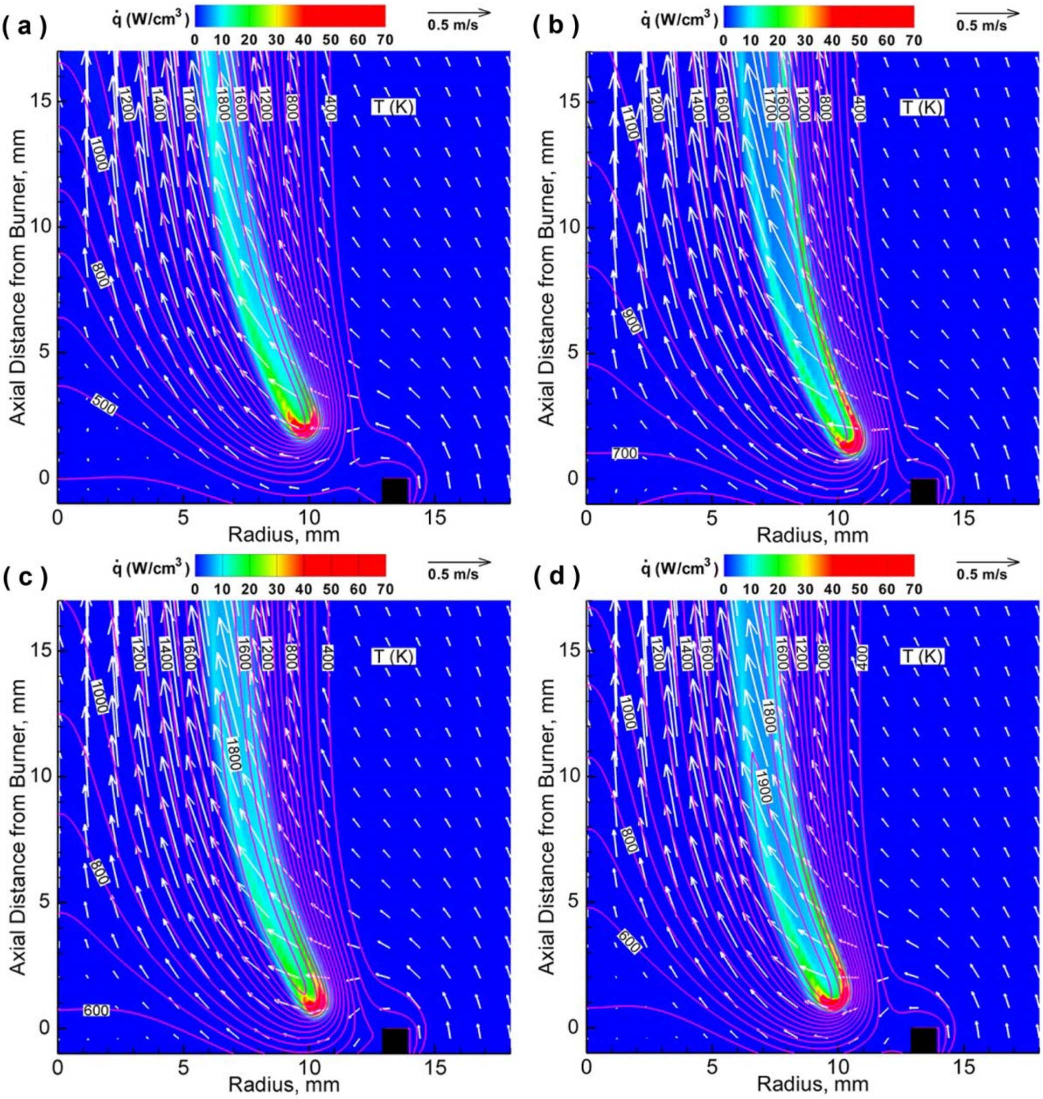


Figure 1. Calculated structure of near-limit propane flames in air with added agent: (a) CF_3Br, X_a=0.0258; (b) C_2HF_5, X_a=0.0765; (c) $C_2HF_3Cl_2$, X_a=0.0455; and (d) $C_3H_2F_3Br$, X_a=0.0246.

Unlike the flame with CF_3Br (Fig. 1a), the heat-release rate contours for the other near-limit flames, particularly with C_2HF_5 (Fig. 1b) and $C_3H_2F_3Br$ (Fig. 1d), show distinct "two-zone" flame structure.

Figure 2 shows the radial variations of the calculated temperature and heat-release rate in propane flames in air with agent: (a) across a trailing flame (z_k + 5 mm); (b) across the reaction kernel: z_k = 1.8 mm (CF_3Br), 1.2 mm (C_2HF_5), 0.8 mm ($C_2HF_3Cl_2$), and 1.4 mm ($C_3H_2F_3Br$). The trailing flames (Fig. 2a) are characterized by the two-zone flame structure (inner and outer) as evident from two heat-release rate peaks most prominently for C_2HF_5 and least significantly for CF_3Br. Although the temperature peak is closer to the inner reaction zone, formed by the hydrocarbon-O_2 combustion, the larger heat-release rate peak for C_2HF_5 is in the outer zone by highly exothermic reactions. The temperature and heat-release-rate profiles in the propane flame with C_2HF_5 (Fig. 2a) are similar to those obtained previously [7] for the ACT fuel with C_2HF_5.

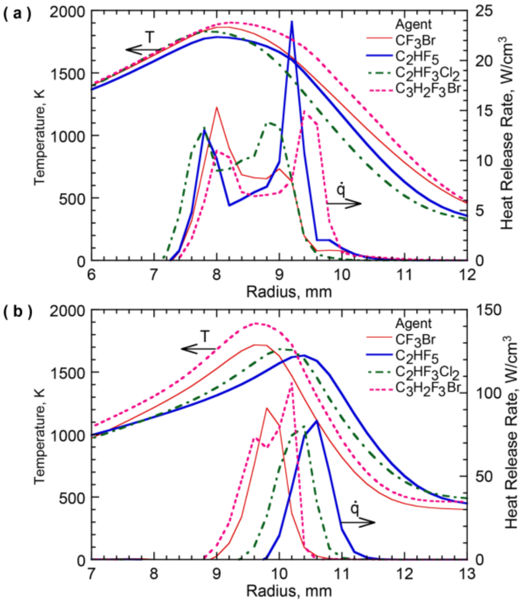


Figure 2. Calculated radial variations of the temperature and heat-release rate in propane flames in air with agent: (a) across a trailing flame (at z_k + 5 mm); (b) across the reaction kernel (at z_k). CF_3Br, X_a = 0.0258, z_k = 1.8 mm; C_2HF_5, X_a = 0.0765, z_k = 1.2 mm; $C_2HF_3Cl_2$, X_a = 0.0455, z_k = 0.8 mm; and $C_3H_2F_3Br$, X_a = 0.0246, z_k = 1.4 mm.

The outer heat-release-rate peak in the trailing flame in $1g_n$ (Fig. 2a) is more evident, compared to the $0g_n$ case [6], due to increased convective fluxes of reactants (i.e., the blowing effect [35]) by the buoyancy-induced incoming flow.

At the reaction kernel in the flame base region (Fig. 2b), the peak heat-release-rate for each agent slightly on the airside of each temperature peak is several times larger than that in the trailing flame. The peak temperature for $C_3H_2F_3Br$ is much higher than other agents, suggesting that additional number of carbon in the agent molecule, compared to CF_3Br, represent potential energy contributions at a fixed concentration.

Figure 3 shows the radial variations of the species volume fractions (X_i) crossing the trailing flame with C_2HF_5 (added at X_a=0.0765) at z= 6.2 mm. Oxygen penetrates through the outer zone and a pool of chain carrier radicals (H, O, and OH) is formed in the middle of the two zones at relatively high concentrations ($X_a \approx 10^{-3}$), thus contributing to both reaction zones. The initial hydrocarbon fuel (C_3H_8) diffuses from the fuel side, decomposes to fragments (CH_4, C_2H_4, and C_2H_2) and reacts with the chain carrier radicals in the inner zone. In the outer zone, the agent (C_2HF_5) from the air side decomposes to many fluorinated species (C_2F_6, CF_2, CHF_3, etc.), which react with the radicals. The H_2O (formed by hydrocarbon-O_2 reaction) diffuses to the outer zone, where it is converted to HF through highly exothermic reactions. The H_2O nearly vanishes in the outer zone in the propane flame, whereas that in the ACT fuel flame with C_2HF_5, reported previously [7], remains at a $X_a \approx 10^{-3}$ level even outside the outer zone due to its high content (X_{H2O} = 0.387) in the fuel. The CF_2O peak (X_{CF2O} = 0.031) in the outer zone in the propane flame is lower than that (X_{CF2O} = 0.048) in the ACT fuel flame. The final products (CO_2, HF, and CF_2O) are distributed radially in a wide range. Low levels of C_2HF_5 on the fuel side and H_2 on the air side in Fig. 3 are due to leakage in the opposite directions through the quenched zone below the flame base. These species' contributions to overall reactions in the opposite zones must be insignificant.

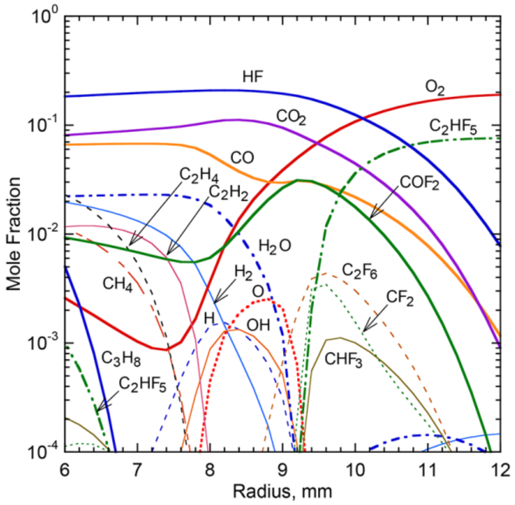


Figure 3. Calculated structure of a propane flame in air with added C_2HF_5 at $X_a = 0.076$ and $z = 5.8$ mm.

Figure 4 shows the radial variations of the calculated production (+) or consumption (-) rates (Fig. 4a) and heat-release rates (Fig. 4b) of species *i* crossing the trailing flame at z=5.8 mm in a propane flame in air with C_2HF_5 at X_a=0.076. In the inner zone, H_2, CO, and the chain carrier radicals (H, O, and OH) are formed and consumed, O_2, and CF_2O are consumed, and H_2O, HF and CO_2 are formed. In the outer zone, C_2HF_5 and O_2 are consumed and HF, CF_2O, and CO are formed. The major contributors to the overall heat-release rate (Fig. 4b) are the formation of H_2O, CO, CO_2 HF in the inner zone, with HF, CF_2O and CO in the outer zone. Although the production rates and heat-release rates of HF and CF_2O in the propane flame are significantly less than those in the ACT fuel flame [7], the resultant heat-release rate profiles are very similar for the two flames. The highly exothermic reactions with the heats of reactions in "( )" include:

$H_2 + OH \rightarrow H + H_2O$ (+61 kJ/mol) (R5)

$CO + OH \rightarrow CO_2 + H$ (+102 kJ/mol) (R61)

$H_2O + F \rightarrow OH + HF$ (+74 kJ/mol) (R1685)

$H_2 + F \rightarrow H + HF$(+135 kJ/mol) (R1679)

$CF_2 + OH \rightarrow CF_2O + H$ (+268 kJ/mol) (R1849)

$CF_3 + OH \rightarrow CF_2O + HF$ (+493 kJ/mol) (R1669)

$CF_2 + O \rightarrow CFO + F$ (+150 kJ/mol) (R1849)

$CF_3 + O \rightarrow CF_2O + F$ (+342 kJ/mol) (R1663)

$CF_3 + H \rightarrow CF_2 + HF$ (+215 kJ/mol) (R1719)

The reactions to form CF_2O are particularly exothermic because of its exceptionally low (negative) heat of formation (-640 kJ/mol).

Figure 5 shows the effects of the agent volume fraction in the coflowing oxidizer on the calculated axial (z_k) and radial (r_k) positions of the reaction kernel from the burner exit on the axis in propane flames. In the present unsteady calculations, as X_a was increased incrementally, the flame-stabilizing reaction kernel in the flame base detached from the burner rim and moved downstream (i.e., the inward and upward direction) gradually and then more steeply as the extinguishment limit approached. For each X_a, a stable stationary flame was obtained.

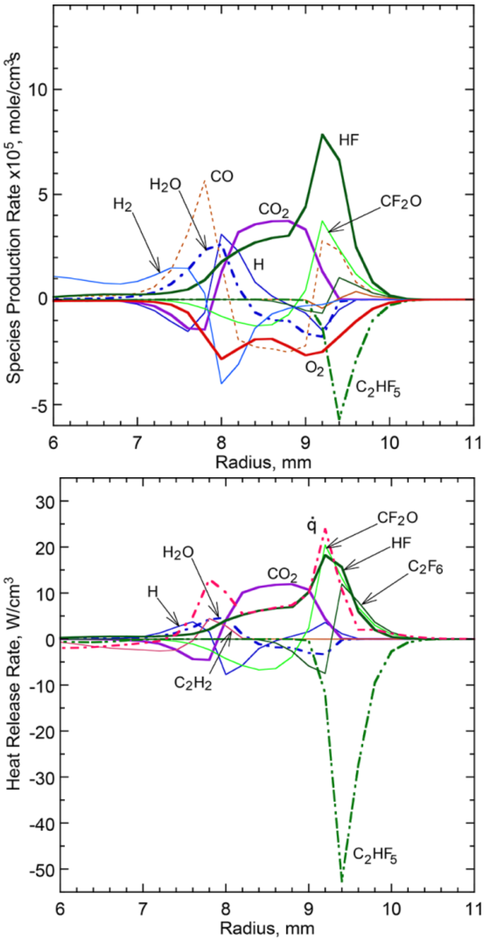


Figure 4. Calculated radial variations of the (a) species production rates, and (b) species and total heat-release rates in a propane flame in air with C_2HF_5 at X_a=0.076 and z=5.8 mm.

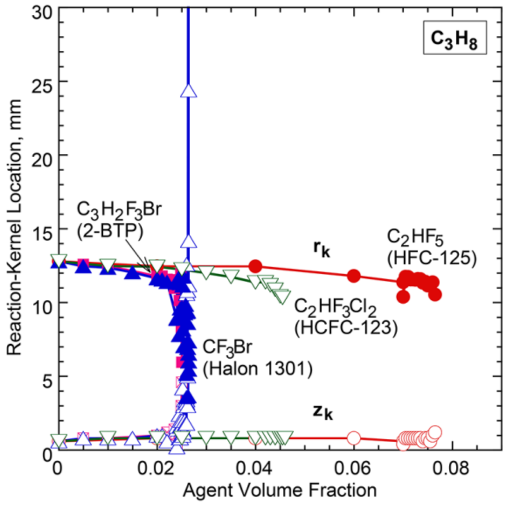


Figure 5. Calculated reaction kernel coordinates of propane flames in air with agent.

For CF_3Br (and, to a lesser extent, C_2HF_5), the flame base oscillated, until finally, blowoff-type extinguishment occurred, whereas for $C_2HF_3Cl_2$ and $C_3H_2F_3Br$, the calculation abruptly diverged at X_a=0.046 and X_a=0.025, respectively. The radial location of the reaction kernel decreased (inward) with X_a, thereby more premixing occurred over the standoff distance. For propane, the MECs of CF_3Br and C_2HF_5 (see Table 1) are: X_a ≈0.04 and ≈0.1, respectively (measured); and X_a=0.0264 and 0.0765, respectively (calculated). By considering technical difficulties, including the stiffness in the computation, complex combustion and inhibition chemistries, and transient blowoff phenomena with occasional flame-base oscillations, the calculated MECs are in fair agreement (≈30 %) with the measurements.

Figure 6 shows the maximum temperature in the trailing diffusion flame and the total heat-release rate ($\dot{q}_{\text{total}}$) integrated over the entire flame and over the flame base region ($\dot{q}_{<\text{zk+3 mm}}$). Thus, both the heat-release rate per unit volume along the flame and the flame size affect $\dot{q}_{\text{total}}$. Unlike chemically passive agents [37, 38], which work thermally to reduce the flame temperature by dilution, the maximum flame temperatures in the present work are nearly constant (≈1800 K) for C_2HF_5 or mildly increased for CF_3Br, $C_3H_2F_3Br$ and $C_2HF_3Cl_2$ as X_a increased until extinguishment. There is a striking difference in $\dot{q}_{\text{total}}$ over the entire flame between CF_3Br and the other agents: $\dot{q}_{\text{total}}$ decreased (i.e., inhibition) with added CF_3Br, whereas it increased (i.e., combustion enhancement) with C_2HF_5 or $C_2HF_3Cl_2$. It is neutral for $C_3H_2F_3Br$. In contrast, for all agents, $\dot{q}_{<\text{zk+3 mm}}$ was nearly constant as X_a increased. Thus, the combustion enhancement occurred only in the trailing flame. In fact, the heat release in the trailing flame ($\dot{q}_{\text{total}}$ - $\dot{q}_{<\text{zk+3 mm}}$) tripled with added C_2HF_5 (at X_a ≈0.08). This enhancement is ≈1.5x larger than the zero-gravity flames studied previously [6], because of much higher incoming flow velocity in normal gravity, resulting in higher reactants (agent and oxygen) influx into the flame zone. Although the volumetric heat-release rate in the trailing flame was an order-of-magnitude smaller than the peak $\dot{q}_{\text{k}}$, integration over the entire trailing flame zone made the total value much larger. This result suggests the significant implication that even if the reaction kernel, with *premixed*-like flame structure, is weakened by halogenated agent addition toward the flame stability limit, the trailing *diffusion* flame can burn more reactants (including the agent itself) because of the additional heat release to form HF and CF_2O in the aforementioned "two-zone" flame structure.

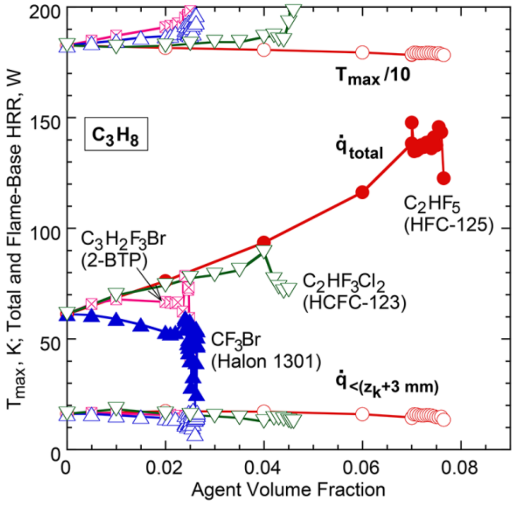


Figure 6. Calculated maximum temperature and total heat release rate (integrated over the entire flame and the base region) in propane flames in air with agent.

CONCLUSIONS

By using propane as the fuel, in addition to the ACT fuel studies previously, the physical and chemical effects of Halon 1301 (CF_3Br) and halon-replacement fire-extinguishing agents (C_2HF_5, $C_2HF_3Cl_2$, and $C_3H_2F_3Br$) are studied numerically to gain better understanding of the flame structure, combustion inhibition/enhancement, and blowoff extinguishment of cup-burner flames. Addition of agent to the coflowing air weakens the flame attachment point (reaction kernel) at the flame base, thereby inducing the detachment, lifting, and blowout extinguishment. With added agent, the calculated maximum flame temperature remains nearly constant (≈1800 K) for C_2HF_5 or mildly increases for CF_3Br, $C_3H_2F_3Br$, and $C_2HF_3Cl_2$. Moreover, the total heat release increases with agent addition for C_2HF_5 and $C_2HF_3Cl_2$ (by up to a factor of 2.5). In the trailing flame, H_2 and H_2O (from hydrocarbon combustion) are converted to HF and CF_2O by exothermic reactions, enhancing an inner flame zone, while reactions of the inhibitor, also forming of HF and CF_2O, created a large outer heat-release zone. In contrast, CF_3Br reduced the total heat release.

ACKNOWLEDGMENTS

This work was supported by The Boeing Company.

REFERENCES

1. Reinhardt, J.W., “Behavior of Bromotrifluoropropene and Pentafluoroethane When Subjected to a Simulated Aerosol Can Explosion,” Federal Aviation Administration, DOT/FAA/AR-TN04/4, 2004.
2. Reinhardt, J.W., “Minimum Performance Standard for Aircraft Cargo Compartment Halon Replacement Fire Suppression Systems (2nd Update),” FAA, DOT/FAA/AR-TN05/20, 2005.
3. Linteris, G.T., Takahashi, F., Katta, V.R., Chelliah, H.K., and Meier, O., "Thermodynamic Analysis of Suppressant-Enhanced Overpressure in the FAA Aerosol Can Simulator," *Fire Safety Science – Proceedings of the Tenth International Symposium*, International Association for Fire Safety Science, Boston, MA, 2011, pp. 1-14.
4. Linteris, G.T., Burgess, D.R., Katta, V.R., Takahashi, F., Chelliah, H.K., and Meier, O., "Stirred Reactor Calculations to Understand Unwanted Combustion Enhancement by Potential Halon Replacements," Combustion and Flame 159: 1016-1025 (2012).
5. Linteris, G.T., Babushok, V.I., Sunderland, P.B., Takahashi, F., Katta, V.R., and Meier, O., "Unwanted Combustion Enhancement by $C_6F_{12}O$ fire Suppressant," Proc. Combust. Institute 34: 2683-2690 (2012).
6. Takahashi, F., Katta, V.R., Linteris, G.T., and Meier, O., “Cup-Burner Flame Structure and Extinguishment by C_2HF_5 in Microgravity,” Proc. of the Combustion Institute 34: 2707-2717 (2012).
7. Takahashi, F., Katta, V.R., Linteris, G.T., and Babushok, V.I., “Combustion Inhibition and Enhancement of Cup-Burner Flames by CF_3Br, C_2HF_5, $C_2HF_3Cl_2$, and $C_3H_2F_3Br$,” Proceedings of the Combustion Institute 35: 2741–2748 (2014).
8. Anon, “Standard on Clean Agent Fire Extinguishing Systems,” National Fire Protection Association, NFPA 2001, Quincy, MA (2000).
9. Anon, Gaseous Fire-Extinguishing Systems Physical Properties and System Design, ISO 14520-Part I, International Organization for Standardization (2000).
10. Sheinson, R.S., Penner-Hahn, J.E., and Indritz, D., “The Physical and Chemical Action of Fire Suppressants,” Fire Safety Journal 15: 437-450 (1989).
11. Hamins, A., Gmurczyk, G., Grosshandler, W., Rehwoldt, R.G., Vazquez, I., Cleary, T., Presser, C., and Seshadri, K., “Flame suppression effectiveness,” in *Evaluation of Alternative In-Flight Fire Suppression for Full Scale Testing in Simulated Aircraft Engine Nacelles and Dry Bays* (W. Grosshandler, R. G. Gann, and W. M. Pitts, Eds.), NIST SP 861, pp. 345-465.
12. Linteris, G.T., “Flame Suppression Chemistry,” in *Advanced Technology for Fire Suppression in Aircraft* (R. G. Gann, Ed.), NIST Special Publication 1069, pp. 119-338, 2007.
13. Linteris, G.T., “Acid Gas Production in Inhibited Propane-Air Diffusion Flames,” in *Halon Replacements: Technology and Science* (A. W. Miziolek and W. Tsang, Eds.), American Chemical Society, Washington, DC, Chap. 19, pp. 225-242, 1995.

14. Linteris, G.T., Takahashi, F., and Katta, V.R., "Fuel Effects in Cup-Burner Flame Extinguishment," 5th US Combustion Meeting, San Diego, March 25-28, 2007.
15. Kim, A., "Overview of Recent Progress in Fire Suppression Technology," National Research Council of Canada, NRCC-45690, 2002.
16. Riches, J., Knutsen, L., Morrey, E., and Grant, K., "A Modified Flame Ionization Detector as a Screening Tool for Halon Alternatives," Halon Alternatives Technical Working Conference, Albuquerque, NM, pp. 115-125, 2000.
17. Grigg, J., Chattaway, A., and Ural, E.A, "Evaluation of Advanced Agent Working Group Agents by Kidde," Halon Options Technical working Conference, Albuquerque, NM, 2001.
18. Katta, V.R., Goss, L.P., and Roquemore, W.M., Numerical Investigations of Transitional H_2/N_2 Jet Diffusion Flames, AIAA Journal 32: 84-94 (1994).
19. Roquemore, W.M., and Katta, V.R., Role of Flow Visualization in the Development of UNICORN, Journal of Visualization 2: 3/4, 257-272 (2000).
20. Barlow, R.S., Karpetis, A.N., Frank, J.H., and Chen, J.-Y., "Scalar Profiles and NO Formation in Laminar Opposed-Flow Partially Premixed Methane/Air Flames," Combustion and Flame 127: 2102-2118 (2001).
21. Fuss, S.P., Hamins, A., "Determination of Planck Mean Absorption Coefficient for HBr, HCl and HF," Transaction ASME 124: 26–29 (2002).
22. Katta, V.R., Forlines, R.A., Roquemore, W.M., Anderson, W.S,. Zelina, J., Goad, J.R., Stouffer, S.D., Roy, S., "Experimental and Computational Study on Partially Premixed Flames in a Centerbody Burner," Combustion and Flame 158: 511-524 (2011).
23. Wang, H., You, X., Jucks, K.W., Davis, S.G., Laskin, A., Egolfopoulos, F., Law, C.K., "USC Mech Version II. High-Temperature Combustion Reaction Model of $H_2/CO/C_1$-C_4 Compounds," available at <http://ignis.usc.edu/USC_Mech_II.htm>, University of Southern California, Los Angeles, CA, 2007.
24. Sheen, D.A., You, X., Wang, H. and Lovas, T., "Spectral Uncertainty Quantification, Propagation and Optimization of a Detailed Kinetic Model for Ethylene Combustion," Proceedings of the Combustion Institute 32: 535–542 (2009).
25. Li, J., Kazakov, A., Chaos, M. , Dryer, F.L., "Chemical Kinetics of Ethanol Oxidation," US Sections/The Combustion Institute Meeting (2007).
26. Li, J., Kazakov, A., F.L. Dryer, "Ethanol pyrolysis experiments in a variable pressure flow reactor," Int. J. Chem. Kinetics 33: 859-867 (2001).
27. Babushok, V.I., Burgess, D.R.F., Tsang, W., and Miziolek, A.W., "Simulation Studies on the Effects of Flame Retardants on Combustion Processes in a Plug Reactor," In *Halon Replacements*, 1995, pp. 275-288.
28. Babushok, V.I., Noto, T., Burgess, D.R.F., Hamins, A., and Tsang, W., "Influence of CF_3I, CF_3Br, and CF_3H on the High-Temperature Combustion of Methane," Combustion and Flame 107: 351-367 (1996).
29. Babushok, V.I., Linteris, G.T., Meier, O.C., and Pagliaro, J.L., Combustion Science and Technology (2014), in press.
30. Pagliaro, J.L., Babushok, V.I., and Linteris, G. T., Combust. Flame (2014), in press.
31. Burgess, D.R., Zachariah, M.R., Tsang, W., and Westmoreland, P.R., "Thermochemical and Chemical Kinetic Data for Fluorinated Hydrocarbons," Progress in Energy and Combust. Sci. 21: 453-529 (1995).
32. Burgess, D., Zachariah, M.R., Tsang, W., and Westmoreland, P.R., "Thermochemical and Chemical Kinetic Data for Fluorinated Hydrocarbons," NIST Technical Note 1412, National Institute of Standards and Technology, Gaithersburg, MD, 1995.
33. Zegers, E.J.P., Williams, B.A., Fisher, E.M., Fleming, J.W., and Sheinson, R.S., "Suppression of Nonpremixed Flames by Fluorinated Ethanes and Propanes," Combust. Flame 121: 471-487 (2000).
34. Takahashi, F., and Katta, V.R., "A Reaction Kernel Hypothesis for the Stability Limit of Methane Jet Diffusion Flames," Proceedings of the Combustion Institute 28: 2071-2078 (2000).
35. Takahashi, F., Linteris, G.T., and Katta, V.R., "Vortex-Coupled Oscillations of Edge Diffusion Flames in Coflowing Air with Dilution," Proceedings of the Combustion Institute 31: 1575-1582 (2007).
36. Takahashi, F., Linteris, G.T., and Katta, V.R., "Extinguishment of Methane Diffusion Flames by Carbon Dioxide in Coflow Air and Oxygen-Enriched Microgravity Environments," Combustion and Flame 155: 37-53 (2008).
37. Takahashi, F., Linteris, G.T., and Katta, V.R., "Extinguishment of Methane Diffusion Flames by Inert Gases in Coflow Air and Oxygen-Enriched Microgravity Environments," Proceedings of the Combustion Institute:33: 2531-2538 (2010).

2016 Spring Technical Meeting
Eastern States Section of the Combustion Institute
Hosted by Princeton University
March 13-16, 2016

Gas-Phase Interactions of Phosphorus Containing Compounds with Cup-Burner Diffusion Flames

Fumiaki Takahashi[1], *Viswanath R. Katta*[2], *Gregory T. Linteris*[3], *Valeri I. Babushok*[3]

[1]*Department of Mechanical and Aerospace Engineering, Case Western Reserve University, Cleveland, Ohio*
[2]*Innovative Scientific Solutions, Inc., Dayton, Ohio*
[3]*National Institute of Standards and Technology, Gaithersburg, Maryland*

The effects of phosphorus-containing compounds (PCC) on the extinguishment and structure of methane-air co-flow diffusion flames, in the cup-burner configuration, have been studied computationally. Dimethyl methylphosphonate (DMMP), trimethyl phosphate (TMP), or phosphoric acid was added to either the air or fuel flow. Time-dependent axisymmetric computation was performed with full gas-phase chemistry and transport to reveal the flame structure and inhibition process. A detailed chemical-kinetics model (77 species and 886 reactions) was constructed by combining the methane-oxygen combustion and phosphorus inhibition chemistry. A simple model for radiation from CH_4, CO, CO_2, and H_2O based on the optically thin-media assumption was incorporated into the energy equation. The two-zone flame structure was formed for DMMP and, to a lesser extent, TMP, due to the heat release by the inhibitor itself. The inhibitor effectiveness was calculated as the minimum extinguishing concentrations (MECs) of CO_2 (added to the oxidizer) as a function of the PCC loading (added to the oxidizer or fuel stream). The calculated MEC of CO_2 without an inhibitor was in good agreement with the measured value. For moderate DMMP loading to the air (<1 %), the measured value became significantly smaller, presumably due to particle formation in the experiment. An inhibitor in the oxidizer flow was an-order-of-magnitude more effective compared to that in the fuel flow in gas-phase inhibition of co-flow diffusion flames.

1. Introduction

Phosphorus-containing compounds (PCCs) are known to be effective at reducing flammability of polymers, with some ambiguity as to whether their effectiveness is due to gas phase reactions involving phosphorus intermediates, or a condensed-phase action [1]. The use of PCCs as fire retardant (FR) additives to plastics has increased dramatically in recent years [2-6]. In this application, the relative importance of gas phase chemistry and solid-phase effects such as char promotion has been debated, with recent work suggesting comparable importance for the two mechanisms, depending on the specific PCC chemistry [3, 7-9]. Due to environmental and health concerns on the most common gas-phase active FR formulations, bromine-containing compounds with antimony trioxide, PCCs are considered as the chemical systems of highest interest to polymer companies and fire retardant manufactures, and the subject of the most

Linteris, Gregory; Takahashi, Fumiaki; Katta, Viswanath; Babushok, Valeri.
"Gas-Phase Interactions of Phosphorus Containing Compounds with Cup-Burner Diffusion Flames."
Paper presented at the Spring 2016 Eastern States Section Meeting of the Combustion Institute, Princeton, NJ, Mar 13-Mar 16, 2016.

intense recent investigations [10, 11]. While FRs added to polymers increase their ignition time and reduce their heat release rates when burning [1, 4, 12], PCCs have also been evaluated as potential halon replacements for fire suppression [13] using cup burner, streaming tests [14, 15] and opposed-jet diffusion flames [16]. Further understanding of how PCCs affect flames is important for their efficient use.

A model for the gas-phase chemical kinetics of phosphorus compounds has been developed over the years. The decomposition of PCCs is a relatively fast, complicated process in a flame reaction zone. Once it has decomposed, PCC's main products (PO_2, PO, HOPO and $HOPO_2$) participate in catalytic radical recombination cycles that inhibit the flame. Simplified versions of the main cycles are shown in Figure 1. Sensitivity and reaction pathway analyses show two main inhibition cycles involving reactions of PO_2, HOPO and $HOPO_2$ species ($PO_2 \Leftrightarrow HOPO$ and $PO_2 \Leftrightarrow HOPO_2$):

(1) $H + PO_2 + M \rightarrow HOPO + M$
$OH + HOPO \rightarrow H_2O + PO_2$
$H + HOPO \rightarrow H_2 + PO_2$
$O + HOPO \rightarrow OH + PO_2$

(2) $OH + PO_2 + M \rightarrow HOPO_2 + M$
$H + HOPO_2 \rightarrow H_2O + PO_2$

Each step of these cycling sequences involves scavenging of H, O, and OH radicals, decreasing their concentration, and correspondingly, the flame reaction rate.

The effects of dimethylmethylphosphonate (DMMP, $PO[CH_3][OCH_3]_2$) in methane-air co-flow diffusion flames, in the cup-burner configuration, have recently been investigated experimentally [17] at the National Institute of Standards and Technology (NIST). By using comprehensive numerical simulations, the present authors have studied the flame structure [18] and inhibition (or combustion enhancement) [19-21] processes in the cup-burner flames. This paper reports the numerical results for three PCCs: DMMP, tetramethylphosphate ($PO[OCH_3]_3$), and phosphoric acid ($PO[OH]_3$). As DMMP and TMP have a significant heating value (due to methyl groups attached to the phosphorus atom), phosphoric acid is also used for a comparison (since it provides the chemical inhibition without the fuel effect). The additive affects the flame structure, which then changes the additive effectiveness. The overall goal of the present work is to understand how the properties of flames interact with the gas-phase inhibition. The knowledge of detailed flame structure that affects fire retardant effectiveness will help to understand the reasons for the variation of effectiveness for phosphorus with flame type.

2. Computational Methods

A time-dependent, axisymmetric numerical code (UNICORN) [22, 23] is used for the simulation of diffusion flames stabilized on the cup burner. A clustered mesh system is employed to trace the gradients in flow variables near the flame surface. The thermo-physical properties such as enthalpy, viscosity, thermal conductivity, and binary molecular diffusion of all of the species are calculated from the polynomial curve fits developed for the temperature range 300 K to 5000 K. Mixture viscosity and thermal conductivity are estimated using the Wilke and Kee expressions, respectively. A simple radiation model based on the optically thin-media assumption for CH_4, CO, CO_2, H_2O and soot is considered. A comprehensive reaction mechanism (77 species and 886 elementary reactions) is assembled from a detailed reaction mechanism of GRI-V3.0 [24] for methane-oxygen combustion and a phosphorus mechanism [25].

The finite-difference forms of the momentum equations are obtained using an implicit QUICKEST scheme [22], and those of the species and energy equations are obtained using a hybrid scheme of upwind and central differencing. A physical domain of 200 mm by 47.5 mm is used with a 351 × 151 non-uniform grid system that yields 0.2 mm by 0.15 mm minimum grid spacing in the *z* and *r* directions, respectively, in the flame zone. The outflow boundary in *z* direction is located sufficiently far from the burner exit ≈14 fuel-cup radii) such that propagation of boundary-induced disturbances into the region of interest is minimal. The cup burner outer diameter is 28 mm and the chimney inner diameter is 95 mm. The burner wall (1-mm long and 1-mm thick tube) temperature is set at 600 K, and the wall surface is under the no-slip velocity condition. The mean gas velocities are set at 1.24 cm/s and 15.5 cm/s, respectively, for the fuel (methane) and oxidizer streams and a temperature of 374 K. The air velocity is in the middle of the so-called "plateau region" [19], where the extinguishing agent concentration is independent of the oxidizer velocity.

Validation of the UNICORN code has been performed for a variety of flame systems, fuels, and inhibitors with the kinetic model used. The predicted global strain rates at extinction of methane-air opposing-jet flames at the reactant temperature of 373 K are 380 s^{-1} without the inhibitor, which is close to the measured value (360 s^{-1}) [16], and those with DMMP added to the flames with different stretch rates are within a range of 10 % of the experiments.

3. Results and Discussion

First, stable flames with an inhibitor were calculated by increasing incrementally (starting at 0) the loading of the inhibitor in the oxidizer or fuel stream. Then, the flame extinguishing conditions were determined by increasing the CO_2 volume fraction (X_{CO2}) in the oxidizer (starting at 0; in increments of < 1 % of X_{CO2} as the limit approached) until the flame blew off. The process was repeated at different inhibitor loadings. Figure 1 shows the calculated and measured [17] inhibitor effectiveness expressed as the MECs of CO_2 added to the oxidizer as a function of the inhibitor loading: (a) added to the oxidizer or (b) fuel stream. The calculated MEC without DMMP was X_{CO2} = 0.199, which was in reasonable agreement (≈ 7 %) with measurement (0.185 at 373 K) [17]. With an addition of DMMP to the oxidizer (Fig. 1a) at very low volume fractions (X_{DMMP-O} <0.003), both measured and calculated MECs of CO_2 decreased rapidly as a result of efficient chemical inhibition. The calculated MEC of CO_2 became significantly larger than the measured value, probably because of particle formation just outside the actual flames with DMMP [17]. Since the calculation did not take into account particle formation, the actual flame temperature could be much lower than the calculation due to the radiative heat loss from the high-temperature particles, formed on the air side of the flame zone [17], thus requiring much lower X_{CO2} at extinguishment. As the DMMP volume fraction was increased further, the rate of decrease (slope) of the MEC curves decreased, particularly for the experiment, and thus the two curves crossed at X_{DMMP-O} = 0.012.

In the experiment [17], the marginal effectiveness of the DMMP diminished, and for X_{DMMP-O} > 0.07, the additional DMMP was essentially ineffective. The behavior for DMMP was very similar to that observed for metallic compounds added to cup-burner flames [18]. The loss of effectiveness for the metals was believed to be due to particle formation (which acted as a sink for the active gas-phase intermediate species that catalytically recombined radicals). Premixed flame structure calculations [17] implied that DMMP addition reduced the concentrations of the chain-carrier radicals (H, O, and OH) to the equilibrium levels so that additional DMMP had little effect on the flame.

The MEC curve for TMP followed closely that for DMMP as the concentrations profiles of the main decomposition products (PO_2, HOPO and $HOPO_2$) were nearly the same. On the other hand, the inhibition effectiveness of phosphoric acid was higher than those of DMMP and TMP. Unlike DMMP and TMP, which have a significant heating value due to methyl groups attached to the phosphorus atom, phosphoric acid provides the chemical inhibition without the fuel effect.

The inhibitor effectiveness of PCCs was reduced markedly when added to the fuel stream (Fig. 1b). As the DMMP volume fraction was increased, the measured MEC of CO_2 decreased rapidly and became nearly ineffective for $X_{\mathrm{DMMP\text{-}F}} > 0.01$. The calculated MEC of CO_2 for DMMP decreased linearly, showing no synergistic effect with CO_2. The volume fraction of DMMP required to extinguish without CO_2 ($X_{\mathrm{DMMP\text{-}F}} = 0.281$) was an order of magnitude larger than that for the addition to the oxidizer ($X_{\mathrm{DMMP\text{-}O}} = 0.0181$).

Figure 2 shows the calculated structure of methane cup-burner flames near extinguishment. The flame with DMMP added to the oxidizer (Fig. 2a) shows the two-zone flame structure [21] due to the heat release by the inhibitor itself on the air side of the main flame zone. There is no outer heat-release zone for DMMP added to the fuel (Fig. 2b). The flame with TMP added to the oxidizer (Fig. 2c) also shows, to a lesser extent, the two-zone flame structure. By contrast, the flame with phosphoric acid added to the oxidizer (Fig. 2d) shows the main flame zone only with relatively high flame temperature. The maximum flame temperature was substantially higher (> 2100 K) for DMMP or TMP added to the oxidizer. The radial distributions of the species volume fractions across the flame base (not shown) revealed that the maximum H-atom concentration decreased to constant values ($X_H \approx 0.0002$ for the PCC loading to the oxidizer, $X_H \approx 0.00024$ for the PCC loading to the fuel).

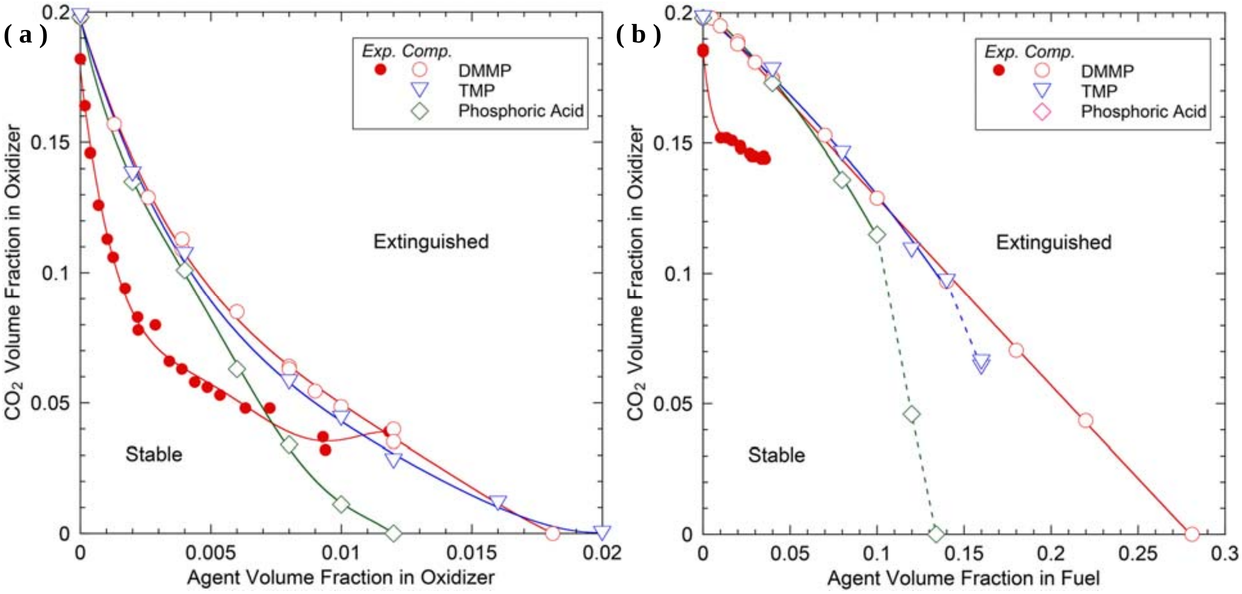


Figure 1 Minimum extinguishing concentrations of CO_2 in methane cup-burner flames: (a) both CO_2 and DMMP added to the oxidizer and (b) CO_2 added to the oxidizer and DMMP to the fuel flow.

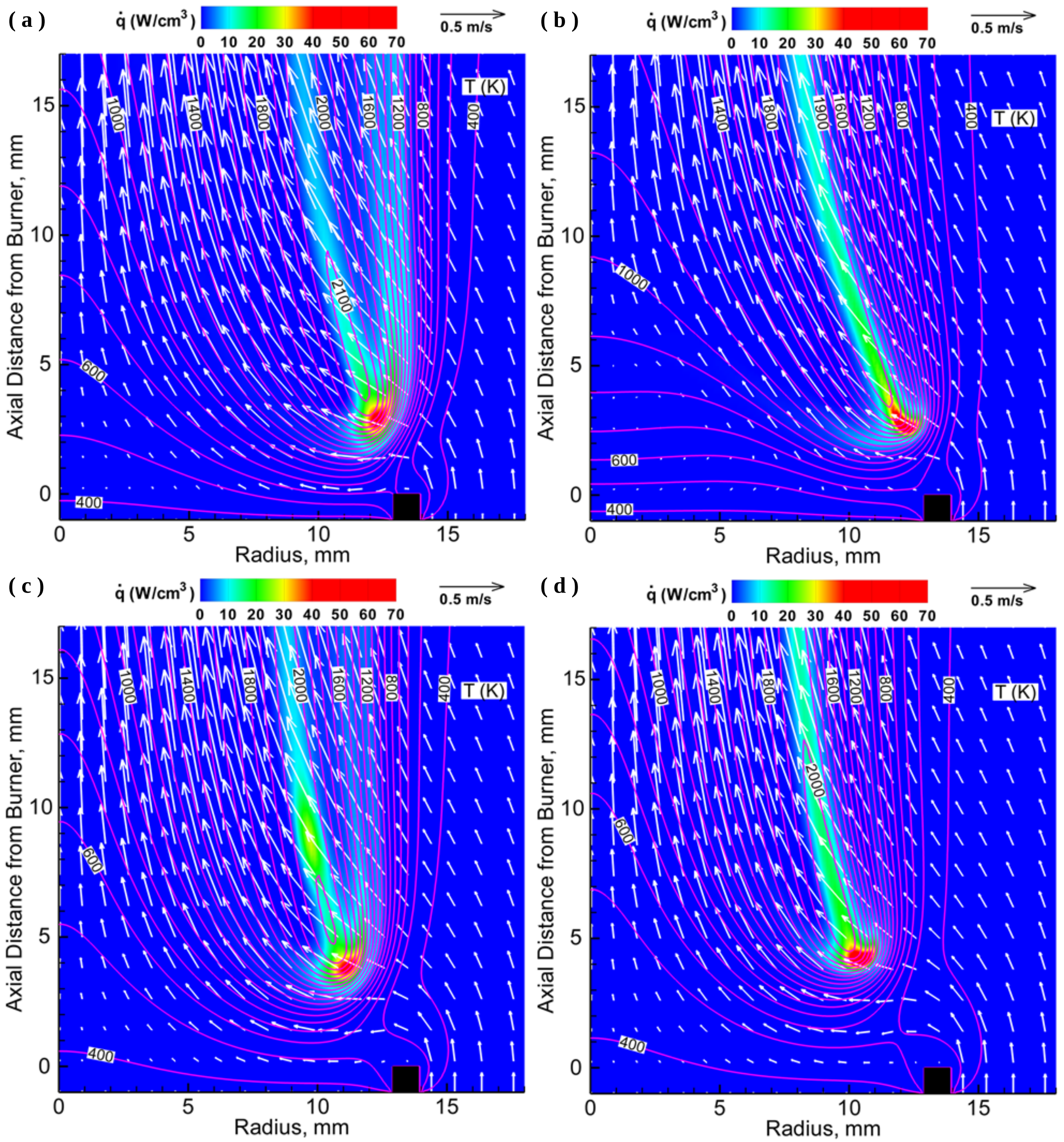


Figure 2: Calculated structure of methane cup-burner flames with agents: (a) DMMP added to the oxidizer at $X_{\mathrm{DMMP\text{-}O}}$ = 0.018, (b) DMMP added to the fuel at $X_{\mathrm{DMMP\text{-}F}}$ = 0.28, (c) TMP added to the oxidizer at $X_{\mathrm{TMP\text{-}O}}$ = 0.016, and (d) phosphoric acid added to the oxidizer at $X_{\mathrm{PA\text{-}O}}$ = 0.011.

Conclusions

The physical and chemical effects of the PCCs, acting in the gas phase, on the structure and inhibition of methane-air co-flow diffusion flames, in the cup-burner configuration, were studied computationally. The inhibitor effectiveness was calculated as the MECs of CO_2 (added to the oxidizer) as a function of the PCC loading (added to the oxidizer or fuel stream). The effectiveness of PCCs added to the oxidizer was high. The two-zone flame structure was predicted with the DMMP (or TMP) addition to the oxidizer due to the reactions of the inhibitor itself. PCCs in the fuel stream were an-order-of-magnitude less effective in gas-phase inhibition of co-flow diffusion flames. This result is a drawback for fire retardants added to solid materials, while it is beneficial to fire suppressants deployed into the surrounding air. The inhibition processes in co-flow diffusion flames are influenced strongly by transport phenomena as well as chemical kinetics because of (1) a small stoichiometric mixture fraction (0.055 for methane), (2) which results in the flame location on the oxidizer side of the dividing streamline, and (3) thus, for the inhibitor added to the fuel, reducing the concentrations of active phosphorus intermediate species (PO_2, HOPO, and $HOPO_2$) in the flame stabilizing region so that the catalytic reactions to recombine the chain-carrier radicals (H, O, and OH) were relatively slow.

Acknowledgements

This work was supported under a Cooperative Agreement between the National Institute of Standards and Technology and FXT Consulting, LLC.

References

[1] G.T. Linteris, Gas-phase Mechanisms of Fire Retardants, NIST IR 6889, NIST, Gaithersburg, MD, 2002.

[2] H. Staendeke D.J. Scharf, Kunststoffe-German Plastics 79 (1989) 1200-1204.

[3] G. Avondo, C. Vovelle, R. Delbourgo, Combust. Flame 31 (1978) 7-16.

[4] S.V. Levchik, Introduction to Flame Retardancy and Polymer Flammability, In: Flame Retardant Polymer Nanocomposites (A.B. Morgan and C.A. Wilkie, eds.), John Wiley & Sons, Inc., 2007, pp.1-29.

[5] L.M. Sherman, Plastics Technol. 38 (1992) 102-105.

[6] S. Shelly, Chem. Eng. 100 (1993) 71-73.

[7] S.K. Brauman, Journal of Fire Retardant Chem. 4 (1977) 18-37.

[8] J. Green, J. Fire Sci. 14 (1996) 426-442.

[9] E.N. Peters, J. Applied Polymer Sci. 24 (1979) 1457-1464.

[10] B. Schartel, Materials 3 (2010) 4710-4745.

[11] S.V. Levchik, and E.D. Weil, J. Fire Sci. 24 (2006) 345-364.

[12] C.P. Fenimore, and G.W. Jones, Combust. Flame 10 (1966) 295-301.

[13] G.T. Linteris, Flame Suppression Chemistry, In: Advanced Technology for Fire Suppression in Aircraft, The Final Report of the Next Generation Fire Suppression Technology Program, NIST SP 1069, 2007, p. 119.

[14] J.A. Kaizerman, and R.E. Tapscott, Advanced Streaming Agent Development, Volume II: Phosphorus Compounds, NMERI 96/5/32540, New Mexico Engineering Research Institute, Albuquerque, NM, 1996.

[15] J.L. Lifke, T.A. Moore, and R.E. Tapscott, Advanced Streaming Agent Development, Volume V: Laboratory-Scale Streaming Tests, NMERI 96/2/32540, NMERI, Albuquerque, NM, 1996.

[16] M.A. McDonald, T.M. Jayaweera, E.M. Fisher, F.C. Gouldin, Combust. Flame 116 (1999) 166-176.

[17] N. Bouvet, G.T. Linteris, V.I. Babushok, F. Takahashi, V.R. Kattta, R.H. Krämer, Fire and Materials, submitted, 2015.

[18] G.T. Linteris, V.R. Kattta, F. Takahashi, Combust. Flame 138 (1-2) (2004) 78-96.

[19] F. Takahashi, G.T. Linteris, V.R. Kattta, Proc. Combust. Inst. 31 (2007) 2721-2729.

[20] F. Takahashi, V.R. Kattta, G.T. Linteris, V.I. Babushok, V.I., Proc. Combust. Inst. 35 (2014).

[21] F. Takahashi, V.R. Kattta, G.T. Linteris, V.I. Babushok, V.I., Fire and Materials, San Francisco, 2015.

[22] V.R. Kattta, L.P. Goss, W.M. Roquemore, AIAA J. 32 (1994) 84.

[23] W.M. Roquemore, V.R. Kattta, J. Visualization 2 3/4 (2000) 257-272.

[24] M. Frenklach, H. Wang, M. Goldenberg, G.P. Smith, D.M. Golden, C.T. Bowman, R.K. Hanson, W.C. Gardiner, V. Lissianski, GRI-Mech—An Optimized Detailed Chemical Reaction Mechanism for Methane Combustion, Report No. GRI-95/0058, Gas Research Institute, Chicago, IL, 1995.

[25] O.P. Korobeinichev, V.M. Shvartsberg, A.G. Shmakov, T.A. Bolshova, T.M. Jayaweera, C.F. Melius, W.J. Pitz, C.K. Westbrook, Proc. Combust. Inst. 30 (2004) 2350-2357.

Numerical Simulations of Gas-Phase Interactions of Phosphorus-Containing Compounds with Cup-Burner Flames

Fumiaki Takahashi, Viswanath R. Katta, Gregory T. Linteris, and
Valeri I. Babushok

Abstract

Computation has been performed for a methane-air co-flow diffusion flame, in the cup-burner configuration, with a phosphorus-containing compound (PCC), dimethyl methylphosphonate (DMMP) or phosphoric acid, added to the oxidizer stream. The time-dependent axisymmetric numerical code, which includes a detailed kinetics model (77 species and 886 reactions), diffusive transport, and a gray-gas radiation model (for CH_4, CO, CO_2, H_2O, and soot), has revealed the interaction of the gas-phase mechanisms of PCCs with the flame structure. The PCCs behave similarly with regard to flame inhibition: both raise the maximum temperature in the trailing flame, lower radical concentrations, and lower the heat-release rate at the peak reactivity spot (i.e., reaction kernel) at the flame base where the flame is stabilized. The mechanism of lowered radical concentrations is primarily due to catalytic cycles involving phosphorus species in both regions of the flame. For DMMP, which contains three methyl groups, the flame exhibited higher temperature and combustion enhancement in the trailing flame, with unique two-zone flame structure.

Keywords

Fire retardant • Fire suppression • Dimethyl methylphosphonate • Phosphoric acid • Diffusion flame structure

1 Introduction

Phosphorus-containing compounds (PCCs) are known to be effective at reducing flammability of polymers, with some ambiguity as to whether their effectiveness is due to gas phase reactions involving phosphorus intermediates, or a condensed-phase action [1]. The use of PCCs as fire retardant (FR) additives to plastics has increased dramatically in recent years [2-6]. In this application, the relative importance of gas phase chemistry and solid-phase effects such as char promotion has been debated, with recent work suggesting comparable importance for the two mechanisms, depending on the specific PCC chemistry [3, 7-9].

Due to environmental and health concerns on the most common gas-phase active FR formulations, bromine-containing compounds, with antimony trioxide usually added as a synergist, PCCs are considered as the chemical systems of highest interest to polymer companies and fire retardant manufactures, and the subject of the most intense recent investigations [10, 11].

While FRs increase their ignition time and reduce their heat release rates when burning [4, 12-13], PCCs have also been evaluated as potential halon replacements for fire

Fumiaki Takahashi
Case Western Reserve University, 10900 Euclid Avenue, Cleveland, OH 44106, USA
e-mail address: fxt13@case.edu

Viswanath R. Katta
Innovative Scientific Solutions, Inc., 7610 McEwen Road, Dayton, OH 45459, USA

Gregory T. Linteris, and Valeri I. Babushok
National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899, USA

The 10th Asia-Oceania Symposium on Fire Science and Technology,

Linteris, Gregory; Takahashi, Fumiaki; Katta, Viswanath; Babushok, Valeri.
"Numerical Simulations of Gas-Phase Interactions of Phosphorus-Containing Compounds with Cup-Burner Flames."
Paper presented at the 10th Asia-Oceania Symposium on Fire Science and Technology (10th AOSFST), Tsukuba, Japan, Oct 5-Oct 7, 2015.

suppression using cup burner, streaming tests [14, 15], and opposed-jet diffusion flames [16]. Further understanding of how PCCs affect flames is important for their efficient use.

A gas-phase chemical kinetics model of phosphorus compounds has been developed [17-22] over the years. Our calculations demonstrate that decomposition of DMMP (or other PCCs) is a relatively fast complicated process in a flame reaction zone. Once it decomposed, its main products (PO_2, PO, HOPO and $HOPO_2$) participate in the cycling sequence of reactions leading to the inhibition influence on the reaction in a flame zone. Figure 1 shows the simplified picture of the main inter-conversions of phosphorus-containing species.

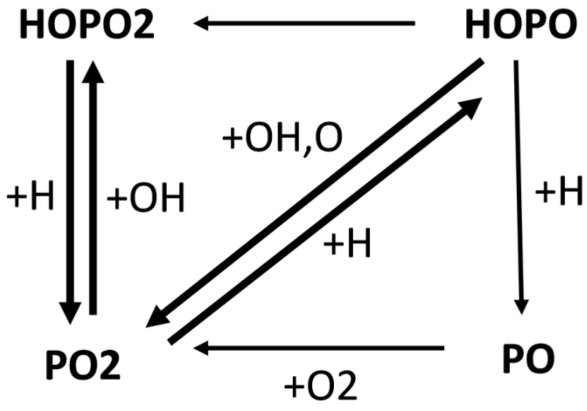


Fig. 1 The abbreviated inhibition reaction cycles of PCC agents.

The sensitivity and reaction pathway analysis show two main inhibition cycles involving reactions of PO_2, HOPO and $HOPO_2$ species ($PO_2 \Leftrightarrow$ HOPO and $PO_2 \Leftrightarrow HOPO_2$):

(1) $H + PO_2 + M \rightarrow HOPO + M$
$OH + HOPO \rightarrow H_2O + PO_2$
$H + HOPO \rightarrow H_2 + PO_2$
$O + HOPO \rightarrow OH + PO_2$

(2) $OH + PO_2 + M \rightarrow HOPO_2 + M$
$H + HOPO_2 \rightarrow H_2O + PO_2$

Each step of these cycling sequences involves a scavenging of H, O, and OH radicals, decreasing the concentration of radical pool, and, correspondingly, decreasing the flame reaction rate.

This mechanism has been used [23-27] to model the inhibition of premixed and counterflow diffusion flames with reasonable results. Nonetheless, no researchers have modeled or extensively studied co-flow diffusion flames, for which poor performance has been observed [16].

The effectiveness of compounds in gaseous flame inhibition is quite complex, depending upon the additive type as well as flame properties. Different inhibitors can be more or less effective depending upon the flame type. Dimethyl methylphosphonate (DMMP, $PO[CH_3][OCH_3]_2$) is about 141 times as effective as CO_2 in a premixed flame [28], 30 times as effective in a counter-flow diffusion flame [16] but only 3 times as effective in a cup-burner flame [29]. For phosphorus, this large variation in effectiveness with flame type has not been explained. Since phosphorous is and will be used as a gas-phase active FR, it would be of great value to understand the conditions for which it is expected to work.

The effects of DMMP in methane-air co-flow diffusion flames, in the cup-burner configuration, have recently been investigated experimentally [30] at the National Institute of Standards and Technology (NIST). The inhibitor effectiveness was measured as the minimum extinguishing concentrations (MECs) of CO_2 (added to the oxidizer) as a function of the DMMP loading (added to the oxidizer or fuel stream), in a similar manner as reported [31] in the literature for n-heptane flames. The particle formation in the flame with added DMMP was studied using the laser scattering technique. In addition, premixed flame simulations were used to approximate the flame chemistry (in the flame stabilization region) at the measured extinguishing conditions [30].

By using comprehensive numerical simulations, the present authors [32, 33] have studied the flame structure and inhibition (or combustion enhancement) processes in the cup-burner flames and, more recently, extended the effort to DMMP [34]. As DMMP has a significant heating value (due to methyl groups attached to the phosphorus atom), phosphoric acid ($PO[OH]_3$) is also used in this report for a comparison (since it provide the chemical inhibition without the fuel effect). The effectiveness of the chemical additive affects the flame structure, which then changes the additive effectiveness, etc. The overall goal of the present work is to understand how the properties of flames interact with the gas-phase inhibition, in support of the experimental research at NIST. The knowledge of detailed flame structure (temperature, species concentration, flow field, etc.) that affects fire retardant effectiveness will help to understand the reasons for the variation of effectiveness for phosphorus with flame type, and to shed light on how fire retardants which act in the gas phase actually retard ignition or reduce heat release. Ultimately, this work aims to aid in the development and application of new compounds that are likely to be used in flame-retarded high-volume thermoplastics to replace the widely used brominated retardants (and their antimony synergist).

2 Computational Methods

A time-dependent, axisymmetric numerical code (UNICORN) [35, 36] is used for the simulation of diffusion flames stabilized on the cup burner. The code solves the axial and radial (z and r) full Navier-Stokes momentum equations, continuity equation, and enthalpy- and species-conservation equations on a staggered-grid system. A clustered mesh system is employed to trace the gradients in flow variables near the flame surface. The thermo-physical properties such as enthalpy, viscosity, thermal conductivity, and binary molecular diffusion of all of the species are calculated from the polynomial curve fits developed for the temperature range 300 K to 5000 K. Mixture viscosity and thermal conductivity are then estimated using the Wilke and Kee expressions, respectively. Molecular diffusion is assumed to be of the binary-diffusion type, and the diffusion velocity of a species is calculated using Fick's law and the effective-diffusion coefficient of that species in the mixture. A simple radiation model based on the optically thin-media assumption is incorporated into the energy equation. Radiation from CH_4, CO, CO_2, H_2O and soot is considered in the present study.

A comprehensive reaction mechanism (77 species and 886 elementary reactions) is assembled and integrated into the UNICORN code for the simulation of methane flames with DMMP added to either the fuel or air stream. A chemical-kinetics model is compiled from a detailed reaction mechanism of GRI-V3.0 [37] for methane-oxygen combustion and a phosphorus mechanism [38] (41 additional species and 448 reactions).

The finite-difference forms of the momentum equations are obtained using an implicit QUICKEST scheme [35], and those of the species and energy equations are obtained using a hybrid scheme of upwind and central differencing. At every time-step, the pressure field is accurately calculated by solving all the pressure Poisson equations simultaneously and using the LU (Lower and Upper diagonal) matrix-decomposition technique.

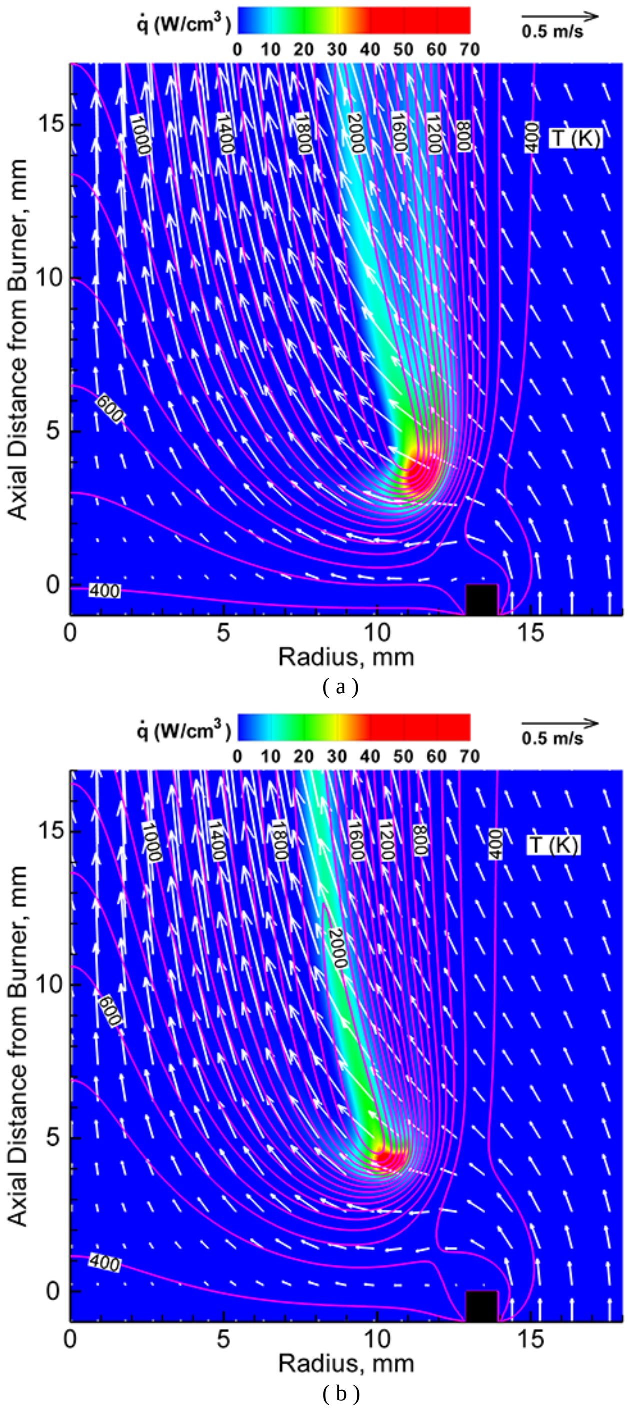
Unsteady axisymmetric calculations for the cup-burner flames are made on a physical domain of 200 mm by 47.5 mm using a 351 × 151 non-uniform grid system that yields 0.2 mm by 0.15 mm minimum grid spacing in the *z* and *r* directions, respectively, in the flame zone. The computational domain is bounded by the axis of symmetry and a chimney wall boundary in the radial direction and by the inflow and outflow boundaries in the axial direction. The outflow boundary in *z* direction is located sufficiently far from the burner exit (~14 fuel-cup radii) such that propagation of boundary-induced disturbances into the region of interest is minimal. Flat velocity profiles are imposed at the fuel and air inflow boundaries, while an extrapolation procedure with weighted zero- and first-order terms is used to estimate the flow variables at the outflow boundary. The cup burner outer diameter is 28 mm and the chimney inner diameter is 95 mm. The burner wall (1-mm long and 1-mm thick tube) temperature is set at 600 K, and the wall surface is under the no-slip velocity condition. The mean gas velocities and temperature are set at 1.24 cm/s and 15.5 cm/s, respectively, for the fuel (methane) and oxidizer streams and 374 K. The low fuel velocity represents low momentum conditions typical of condensed material fires. The air velocity is in the middle of the so-called “plateau region” [32], where the extinguishing agent concentration is independent of the oxidizer velocity.

Validation of the UNICORN code has been performed for a variety of flame systems, fuels, and inhibitors with the kinetic model used. The predicted global strain rates at extinction of methane-air opposing-jet flames at the reactant temperature of 100 °C are 380 s^{-1} without the inhibitor, which is close to the measured value (360 s^{-1}) [16], and those with DMMP added to the flames with different stretch rates are within a range of 10 % of the experiments.

3 Results and Discussion

The numerical simulations reported previously [39, 40] show that the flame-base region supports a trailing flame and controls the flame attachment, detachment, and oscillation processes. Near the extinguishment limit, small variations in the agent volume fraction in the oxidizing stream result in profound changes in the flame structure. The calculated inner structure of the flame base region provides detailed physical and chemical insights into the flame stabilizing mechanism and inhibition processes.

Figure 2 shows the calculated structure of near-limit flames in air with (a) DMMP at $X_{DMMP\text{-}O}$ = 0.012 and CO_2 at X_{CO2} = 0.032 (Fig. 2a) and (b) $PO(OH)_3$ at $X_{PO(OH)3\text{-}O}$ = 0.011 (with no CO_2 added) (Fig. 2b). The variables include the velocity vectors (***v***), isotherms (*T*), and heat-release rate ($\dot{q}$). Although unsteady code is used, the calculated flames are nearly steady state without flame flickering or base oscillations throughout the entire process because of the relatively high oxidizer flow velocity and temperature. The base of both flames is detached and lifted above the burner rim at the height from the burner rim, z_k = 3.4 mm (Fig. 2a) and 4.2 mm (Fig. 2b) in the nearly horizontal entrainment flow. The velocity vectors show longitudinal acceleration in the hot zone due to buoyancy. As a result of the continuity of the fluid, surrounding air is entrained into the lower part of the flame. The entrainment flow inclines inwardly as a result of the overall stream-tube (streamline spacing) shrinkage due to the significantly low velocity of the fuel compared to that of the oxidizer as well as the flow



(a)

(b)

Fig. 2 Calculated structure of methane cup-burner flames with agents added to the oxidizer: (a) DMMP at X_{DMMP-O} = 0.012, X_{CO2} = 0.032 and (b) PO(OH)$_3$ at $X_{PO(OH)3-O}$ = 0.011.

acceleration downstream. The heat-release rate contours show a peak reactivity spot (i.e., the reaction kernel [39]) at the flame base, where the chain-carrier radicals (H, O, and OH), as well as heat, diffuse back against the oxygen-rich incoming buoyancy-induced flow, thus promoting chain-branching (H + O$_2$ → OH + O) and subsequent vigorous reactions to form the reaction kernel.

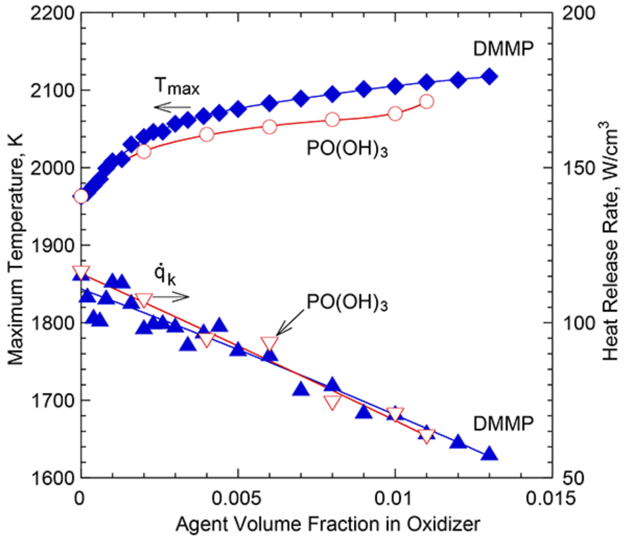


Fig. 3 Calculated maximum temperature and reaction-kernel heat-release rate in methane cup-burner flames with DMMP or PO(OH)$_3$ added to the oxidizer.

For DMMP (Fig. 2a), the heat-release rate contour shows a weak branch on the oxidizer side extending downstream from the reaction kernel. This feature was similar to the two-zone flame structure for halon replacement fire-extinguishing agents with fuel components, as found previously [33]. The two-zone flame structure is formed due to burning of the fuel component of DMMP, while for PO(OH)$_3$, no outer branch is formed.

Figure 3 shows the maximum temperature in the trailing diffusion flame and the peak heat-release rate at the reaction kernel in the flame with pure DMMP or PO(OH)$_3$ in the oxidizer. As DMMP or PO(OH)$_3$ is added to the oxidizer, T_{max} increases, whereas the reaction kernel weakens (the heat-release rate decreases linearly). T_{max} in the trailing flame with DMMP added to the oxidizer is higher than that with PO(OH)$_3$ possibly due to combustion enhancement by additional heat release.

Figure 4 shows the radial variations of calculated temperature and the heat-release rate crossing the reaction kernel at z_k = 3.4 mm and the trailing flame at z = 6.4 mm (z_k + 3 mm) in the near-limit flame with DMMP at X_{DMMP-O} = 0.012 and CO$_2$ at X_{CO2} = 0.032 (see Fig. 2a). At z_k = 3.4 mm, the heat-release rate peak resides slightly on the oxidizer side of the temperature peak, as the reaction kernel broadens as a result of fuel-air mixing in the region between the flame base and the burner rim. At z = 6.4 mm, the trailing diffusion flame is characterized by "two-zone" structure [33] (inner and outer) as evident from two heat-release rate peaks. The inner zone (10 mm < r < 11.4 mm) is formed by the hydrocarbon-O2 combustion with the

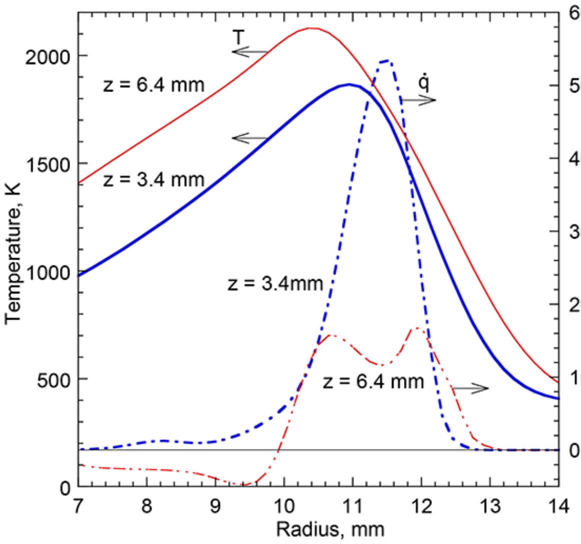
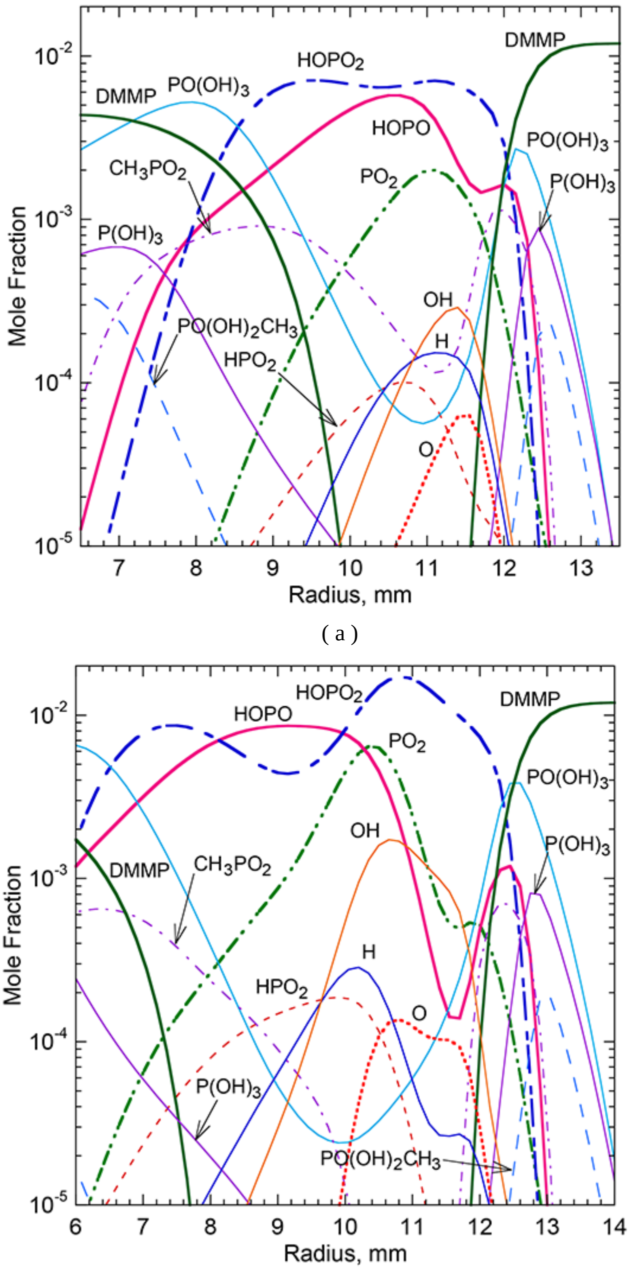


Fig. 4 Calculated radial variations of the temperature and heat-release rate at z = 3.4 mm and 6.4 mm in a methane cup-burner flame with DMMP and CO2 added to the oxidizer at $X_{\mathrm{DMMP\text{-}O}}$ = 0.012 and X_{CO2} = 0.032, respectively.

heat-release rate peak residing on the temperature peak. The outer zone (11.4 mm < r < 13 mm) is formed by exothermic reactions of the retardant itself.

Figure 5 shows the radial variations of the volume fractions (X_i) of phosphorus-containing species and the chain-carrier radicals (H, O, and OH) crossing the reaction kernel at z_k = 3.4 mm (Fig. 5a) and the trailing flame at z_k = 6.4 mm (Fig. 5b) with DMMP added at $X_{\mathrm{DMMP\text{-}O}}$ = 0.012 and CO_2 at X_{CO2} = 0.032. In the region surrounding the reaction kernel (Fig. 5a), DMMP in the oxidizer stream reacts with O_2 and the radicals and is fragmented and diminished. As a result, the concentration peaks of species such as $PO(OH)_3$, CH_3PO_2, and $P(OH)_3$ are formed in this peripheral region. Relatively high concentrations (X_i in the order of 10^{-3}) of active phosphorus intermediates ($HOPO_2$, HOPO, and PO_2) present in the high-temperature central region, where the peaks of the chain-carrier radicals (H, O, and OH) are formed. Consequently, the afore-mentioned phosphorus inhibition reactions of radical recombination cycles are taking place vigorously at the reaction kernel. In the trailing flame (Fig. 5b), as a result of the two-zone flame structure and higher temperature, the DMMP fragments, active phosphorus intermediates, and radicals spread radially at higher concentrations.

Figure 6 shows the radial variations of calculated temperature and the heat-release rate crossing the reaction kernel at z_k = 4.2 mm and the trailing flame at z = 7.2 mm (z_k + 3 mm) in the near-limit flame with $PO(OH)_3$ at $X_{\mathrm{PO(OH)3\text{-}O}}$ = 0.011 (see Fig. 2b). As described above, no outer zone with a significant heat-release rate peak is formed in the trailing flame.



(a)

(b)

Fig. 5 Calculated radial variations of the volume fractions in a methane cup-burner flame with DMMP and CO2 added to the oxidizer at $X_{\mathrm{DMMP\text{-}O}}$ = 0.012 and X_{CO2} = 0.032, respectively, at (a) z = 3.4 mm and (b) z = 6.4 mm.

Figure 7 shows the radial variations of the volume fractions (X_i) of phosphorus-containing species and the chain-carrier radicals (H, O, and OH) crossing the reaction kernel at z_k = 4.2 mm (Fig. 7a) and the trailing flame at z_k = 7.2 mm (Fig. 7b) with $PO(OH)_3$ added at $X_{\mathrm{PO(OH)3\text{-}O}}$ = 0.011. At both z_k = 4.2 mm and 7.2 mm, the volume fractions of phosphorus intermediates on the air side of the

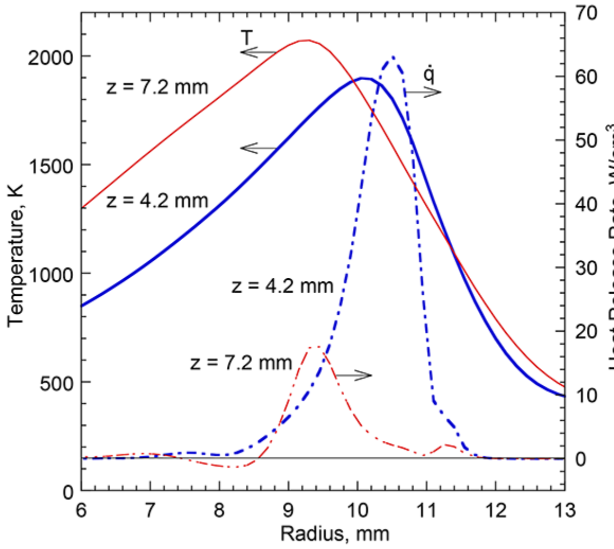


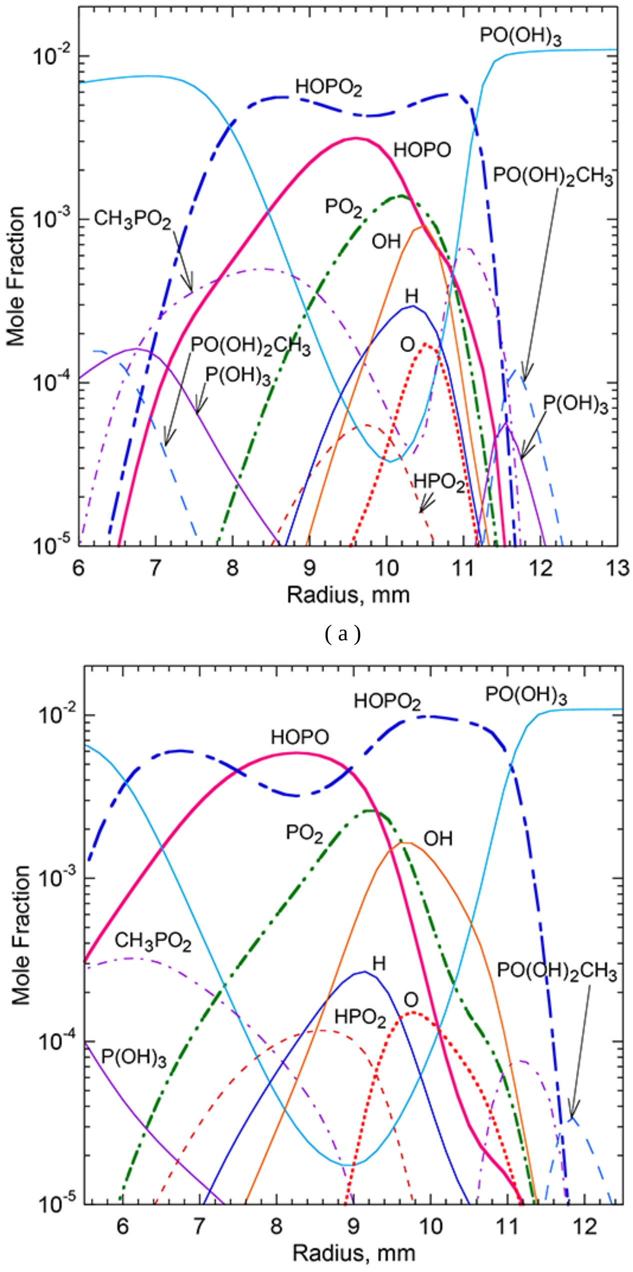
Fig. 6 Calculated radial variations of the temperature and heat-release rate at z = 4.2 mm and 7.2 mm in a methane cup-burner flame with PO(OH)$_3$ added to the oxidizer at $X_{PO(OH)3\text{-}O}$ = 0.011.

temperature peak are much smaller than the DMMP addition (Fig. 4).

The effectiveness of phosphorus compounds in inhibition is quite complex, depending on the additive type and the flame structure, which depends on the region in the flame. As shown in Fig. 3, the PCC addition to the oxidizer results in higher T_{max}, which would increase the radical concentrations. On the other hand, the two-zone flame structure with DMMP generates more active phosphorus intermediates on the oxidizer side of the trailing flame, thus promoting the radical recombination cycles. In the reaction kernel, there is good upstream mixing of fuel and oxidizer because the base is lifted. Thus, the inhibition characteristics in the reaction kernel must be closer to those in premixed flames, where the species for the catalytic cycles are more readily available.

4 Conclusions

The effects of the PCCs (DMMP and PO[OH]$_3$) acting in the gas phase on the structure and inhibition of methane-air co-flow cup-burner flames have been studied computationally. The two-zone flame structure has been calculated with the DMMP addition to the oxidizer due to the reactions of the retardant itself, whereas PO[OH]$_3$ lacks it. The effectiveness of PCCs added to the oxidizer is outstanding. Although the PCCs in the oxidizer increased the maximum flame temperature, particularly for DMMP, in the trailing diffusion flame, it weakened the flame attachment point (reaction kernel) at the flame base, thereby inducing the detachment, lifting, and blowout extinguishment.



(a)

(b)

Fig. 7 Calculated radial variations of the volume fractions in a methane cup-burner flame with PO(OH)$_3$ added to the oxidizer at $X_{PO(OH)3\text{-}O}$ = 0.011, at (a) z = 4.2 mm and (b) z = 7.2 mm.

Acknowledgement This work was supported under the Cooperative Agreement by the National Institute of Standards and Technology with FXT Consulting, LLC.

References

[1] Linteris, G.T., 2007, Flame Suppression Chemistry, In: Advanced Technology for Fire Suppression in Aircraft, The Final Report of the Next Generation Fire Suppression Technology Program (R.G. Gann, Ed.), NIST Special Publication 1069,

National Institute of Standards and Technology, Gaithersburg, MD, pp. 119-338.

[2] Staendeke, H. and Scharf, D.J., 1989, Halogen-Free Flame-Retardant Based on Phosphorus-Compounds, Kunststoffe-German Plastics 79, 1200-1204.

[3] Avondo, G., Vovelle, C., and Delbourgo, R., 1978, Role of Phospohorus and Bromine in Flame Retardancy, Combustion and flame 31, pp. 7-16.

[4] Levchik, S.V., 2007, Introduction to Flame Retardancy and Polymer Flammability, In: Flame Retardant Polymer Nanocomposites (A.B. Morgan and C.A. Wilkie, eds.), John Wiley & Sons, Inc., pp.1-29.

[5] Sherman, L.M., 1992, Flame Retardants Update: Phosphorus Expands Its Niche, Plastics Technology 38, pp. 102-105.

[6] Shelly, S., 1993, Keeping Fire at Bay, Chemical Engineering 100, pp. 71-73.

[7] Brauman, S.K., 1977, Phosphorus Fire Retardance in Polymers. I. General Mode of Action, Journal of Fire Retardant Chemistry 4, pp. 18-37.

[8] Green, J., 1996, Mechanisms for Flame Retardancy and Smoke Suppression: A Review, Journal of Fire Sciences 14, pp. 426-442.

[9] Peters, E.N., 1979, Flame-Retardant Thermoplastics. 1. Polyethylene-Red Phosphorus, Journal of Applied Polymer Science 24, pp. 1457-1464.

[10] Schartel, B., 2010, Phosphorus-based Flame Retardancy Mechanisms-Old Hat or a Starting Point for Future Development?, Materials 3, pp. 4710-4745.

[11] Levchik, S.V. and Weil, E.D., 2006, A Review of Recent Progress in Phosphorus-Based Flame Retardants, Journal of Fire Science 24, pp. 345-364. General Mode of Action, Journal of Fire Retardnt Chemistry 4, pp. 18-37.

[12] Fenimore, C.P, and Jones, G.W., 1966, Modes of Inhibiting Polymer Flammability, Combustion and Flame 10 pp. 295-301.

[13] Linteris, G.T., 2002, Gas-phase Mechanisms of Fire Retardants, NIST IR 6889, National Institute of Standards and Technology, Gaithersburg, MD.

[14] Kaizerman, J.A., and Tapscott, R.E., 1996, Advanced Streaming Agent Development, Volume II: Phosphorus Compounds, NMERI 96/5/32540, New Mexico Engineering Research Institute, Albuquerque, NM.

[15] Lifke, J.L., Moore, T.A., and Tapscott, R.E., 1996, Advanced Streaming Agent Development, Volume V: Laboratory-Scale Streaming Tests, NMERI 96/2/32540, New Mexico Engineering Research Institute, Albuquerque, NM.

[16] McDonald, M.A., Jayaweera, T.M., Fisher, E.M., and Gouldin, F.C., 1999, Inhibition of Nonpremixed flames by Phophorus-Containing Compounds, Combustion and Flame 116, 166-176.

[17] Hastie J.W., and Bonnell D.W., 1980, Molecular Chemistry of Inhibited combustion Systems, NBSIR 80-2169, National Bureau of Standards, Gaithersburg, MD.

[18] Twarowski, A., 1993, The Influence of Phosphorus Oxides and Acids on the Rate of H+OH Recombination, Combustion and Flame 94, pp. 91-107.

[19] Werner, J.H., and Cool, T.A., 1999, Kinetic Model for the Decomposition of DMMP in a hydrogen/Oxygen Flame, Combustion and Flame 117, pp. 78-98.

[20] Babushok, V.I., and Tsang, W, 1999, Influence of Phosphorus-Containing Fire Suppressants on Flame Propagation, In: Society of Fire Protection Engineers, Boston, MA.

[21] Wainner, R.T., McNesby, K.L., Daniel, R.G., Miziolek, A.W., and Babushok, V.I., 2000, Experimental and Mechanistic Investigation of Opposed-Flow Propane/Air Flames by Phosphorus-Containing Compounds, Proceedings of the Halon Options Technical Working Conference (HOTWC), Albuquerque, NM, May 2-4, pp 141-153.

[22] Glaude, P.A., Curran, H.J., Pitz, W.J. Westbrook, C.K., 2000, Kinetic Study of the Combustion of Orgnophophorus Compounds, Proceedings of the Combustion Institute 28, pp. 1749-1756.

[23] McDonald, M.A., Gouldin, F.C., and Fisher, E.M., 2001, Temperature Dependence of Phosphorus-Based Flame Inhibition, Combustion and Flame 124, pp. 668-683.

[24] Korobeinichev, O.P., Bolshova, T.A., Shvartsberg, V.M., and Chernov, A.A., 2001, Inhibition and Promotion of Combustion by Organophosphorus Compounds Added to Flames of CH4 or H2 in O2 and Ar, Combustion and Flame 125, pp. 744-751.

[25] Korobeinichev, O.P., Rybitskaya, I.V., Shmakov, A.G., Chernov, A.A., Bolshova, T.A., and Shvartsberg, V.M., 2009, Inhibition of Atmospheric-Pressure $H_2/O_2/N_2$ Flames by Trimethyl-Phosphate Over Range of Equivalence Ratio, Proceedings of the Combustion Institute 32, pp. 2591-2597.

[26] Korobeinichev, O.P., Rybitskaya, I.V., Shmakov, A.G., Chernov, A.A., Bolshova, T.A., and Shvartsberg, V.M., 2010, Mechanism of Inhibition of Hydrogen/Oxygen Flames of Various Compositions by Trimethyl Phosphate, Kinetics and Catalysis 51, pp.154-161.

[27] Bolshova, T.A., and Korobeinichev, O.P., 2006, Promotion and Inhibition of a Hydrogen-Oxygen Flame by the Addition of Trimethyl Phosphate, Combustion Explosion and Shock Waves 42, pp. 493-502.

[28] Korobeinichev, O., Mamaev, A., Sokolov, V., Bolshova, T., Shvartsberg, V., Zakharov, L., and Kudravtsev, I., 2000, Inhibition of Methane Atmospheric Flames by Organophosphorus Compounds, Halon Options Technical Working Conference, Albuquerque, NM, May 2-4, pp. 164-172.

[29] Tapscott, R.E., Mather, J.D., Heinonen, E.W., Lifke, J.L., and Moore, T.A., 1998, Identification and Proof Testing of New Total Flooding Agents: Combustion Suppression Chemistry and Cup-Burner Testing, NMERI 97/6/33010, Albuquerque, NM: New Mexico Engineering Research Institute.

[30] Bouvet, N., Linteris, G.T., Babushok, V.I., Takahashi, F., Katta, V.R., and Krämer, R.H., 2015, Experimental and Numerical Simulations of the Gas-Phase Effectiveness of Phosphorus Compounds, Fire and Materials 2015, Interscience Communications Ltd, London, UK.

[31] Shmakov, A.G., Korobeinichev, O.P., Shvartsberg, V.M., Knyazkov, D.A., Bolshova, T.A., and Rybitskaya, I.V., 2005, Inhibition of Premixed and Nonpremixed Flames with Phosphorus-Containing Compounds, Proceedings of the Combustion Institute 30, pp. 2345-2352.

[32] Takahashi, F., Linteris, G., and Katta, V.R., 2007, Extinguishment Mechanisms of Coflow Diffusion Flames in A Cup-Burner Apparatus, Proceedings of the Combustion Institute 31, pp. 2721-2729.

[33] Takahashi, F., Katta, V.R., Linteris, G.T., and V.I. Babushok, V.I., 2014, Combustion Inhibition and Enhancement of Cup-Burner Flames by CF_3Br, C_2HF_5, $C_2HF_3Cl_2$, and $C_3H_2F_3Br$, Proceedings of the Combustion Institute 35.

[34] Takahashi, F., Katta, V.R., Linteris, G.T., and Babushok, V.I., 2015, Simulations of Gas-Phase Interactions of Phosphorus Flame Retardants with Diffusion Flame Structure, Fire and Materials 2015, Interscience Communications Ltd, London, UK.

[35] Katta, V.R., Goss, L.P., and Roquemore, W.M., 1994, Numerical investigations of transitional H2/N2 jet diffusion flames, AIAA Journal 32, p. 84.

[36] Roquemore, W.M., and Katta, V.R., 2000, Role of Flow Visualization in the Development of UNICORN. Journal of Visualization 2, ¾, pp. 257-272.

[37] Frenklach, M., Wang, H., Goldenberg, M., Smith, G.P., Golden, D.M., Bowman, C.T., Hanson, R.K., Gardiner, W.C., Lissianski, V., 1995, GRI-Mech—An Optimized Detailed Chemical Reaction Mechanism for Methane Combustion, Report No. GRI-95/0058, Gas Research Institute, Chicago, IL.

[38] Korobeinichev, O.P., Shvartsberg, V.M., Shmakov, A.G., Bolshova, T.A., Jayaweera, T.M., Melius, C.F., Pitz, W.J. and Westbrook, C.K., 2004, Flame Inhibition by Phosphorus-Containing Compounds in Lean and Rich Propane Flames, Proceedings of the Combustion Institute 30, pp. 2350-2357.

[39] Takahashi, F., and Katta, V.R., 2000, A Reaction Kernel Hypothesis for the Stability Limit of Methane Jet Diffusion Flames, Proceedings of the Combustion Institute 28, 2071-2078.

[40] Takahashi, F., Linteris, G.T., and Katta, V.R., 2007, Vortex-Coupled Oscillations of Edge Diffusion Flames in Coflowing Air with Dilution, Proceedings of the Combustion Institute 31, pp. 1575-1582.

A PROBABILISTIC NETWORK FORENSIC MODEL FOR EVIDENCE ANALYSIS

Changwei Liu[#1], Anoop Singhal[*2], Duminda Wijesekera[#,*3]
[#]Department of Computer Science, George Mason University, Fairfax VA 22030 USA
[1]cliu6@gmu.edu, [3]dwijesek@gmu.edu
[*]National Institute of Standards and Technology, Gaithersburg MD 20899 USA
[2]anoop.singhal@nist.gov

Abstract: Modern-day attackers tend to use sophisticated multi-stage/multi-host attack techniques and anti-forensics tools to cover their attack traces. Due to the current limitations of intrusion detection systems (IDS) and forensic analysis tools, the evidence can be a false positive or missing. Besides, the number of security events is so large that finding an attack pattern is like finding a needle in a haystack. Under this situation, reconstructing the attack scenario that can hold the attacker accountable for their crime is very challenging.

This paper describes a probabilistic model that applies Bayesian Network to constructed evidence graphs, systematically addressing how to resolve some of the above problems by detecting false positives, analyzing the reasons of the missing evidence and computing the probability for an entire attack scenario. We have also developed a software tool based on this model for network forensics analysis. Our system is based on a Prolog system using known vulnerability databases and an anti-forensics database that is similar to the NIST National Vulnerability Database (NVD). Our experimental results and case study show that such a system can be useful for constructing the most likely attack scenario and managing errors for network forensics analysis.

Keywords: Network forensic, Digital evidence, Logical evidence graphs, Bayesian Network

Liu, Changwei; Singhal, Anoop; Wijesekera, Duminda.
“A Probabilistic Network Forensics Model for Evidence Analysis.”
Paper presented at the IFIP Advances in Information and Communication Technology, New Delhi, India, Jan 4-Jan 6, 2016.

1. INTRODUCTION

Digital forensics investigators use evidence and contextual facts to formulate attack hypotheses, and assess the probability that the facts support or refute their hypotheses on network attacks [7]. However, due to limitation of forensic tools and expert's opinions, in an enterprise network, formalizing a hypothesis and providing quantitative measures to support the hypothesis on multi-step, multi-host attacks is a challenge. As a solution, we designed a method and developed a software tool to partially automate the process of constructing quantitatively supportable attack scenarios using the available evidence. We show its applicability with a case study.

Our method uses Bayesian Network (BN) to estimate the likelihood and false positive rates of potential attack scenarios that fit discovered evidence. Although Bayesian Networks have been used for digital evidence modeling [5,6,7,12], to the best of our knowledge, the above contributions construct BNs in an ad hoc manner. In this paper, we show how our method automate the process of organizing evidence in a graph structure (that we call a logical evidence graph) and applying Bayesian analysis to the entire graph. By doing so, the system can: (1) provide us attack scenarios with acceptable false positive rates, and (2) dynamically update joint posterior attack probability and false positive rate of an attack path when new evidence along the attack path is presented.

The rest of this paper is organized as follows. Section 2 provides background and related work. Section 3 describes Logical evidence Graphs. Section 4 describes our probabilistic analysis. Section 5 describes a case study. Section 6 concludes the paper.

2. BACKGROUND AND RELATED WORK

Bayesian Networks have been used to facilitate the expression of opinions regarding legal determinations on the credibility and relative weight of non-digital evidence [5, 6, 7, 8, 12]. In criminal forensics, many researchers use BNs to model dependencies between hypothesis and evidence taken from crime scenes and use these models to update belief probability of newly found evidence given the previous ones [5, 6, 8, 10,11, 12]. Digital forensics researchers also have used BNs to reason about evidence in order to quantify their "strengths" in supporting hypotheses about reliability and traceability [7]. However, in the above work, BNs were custom-built without using a uniform model. Also, tools that directly support automatically building a Bayesian Network from available evidence and estimating belief probabilities and corresponding potential error rate given the evidence have been minimal.

Our system is based on a Prolog-based reasoning system MulVAL [13,14] using known vulnerability databases and an anti-forensics database that we plan to extend to a standardized database like the NIST National Vulnerability Database (NVD).

3. LOGICAL EVIDENCE GRAPHS

This section defines evidence graphs and shows how we design rules to correlate available evidence to attack scenarios. Because we use reasoning to link observed attack events and collected evidence, we call them logical evidence graphs.

Definition 1 (Logical Evidence Graph- LEG): LEG=(N_r,N_f,N_c,E,L,G) is said to be a logical evidence graph (LEG), where N_f, N_r and N_c are three sets of disjoint nodes in the graph (called fact, rule, and consequence fact nodes respectively), $E \subseteq ((N_f \cup N_c) \times N_r) \cup (N_r \times N_c))$, and L is a mapping from a node to its labels. $G \subseteq N_c$ are the observed attack events. Every rule node has a consequence fact node as its single child and one or more fact or consequence fact nodes from prior attack steps as its parents. Node labels consist of instantiations of rules or sets of predicates specified as follows:

1. A node in N_f is an instantiation of predicates that codify system state including access privileges, network topology consisting interconnectivity information, or known vulnerabilities associated with host computers in the system. We use the following predicates:

   a. "hasAccount(_principal, _host, _account)", "canAccessFile(_host, _user, _access, _path)" and etc. to model access privileges.

   b. "attackerLocated(_host)" and "hacl(_src, _dst, _prot, _port)" to model network topology, namely, the attacker location and network reachability information.

   c. "vulExists(_host, _vulID, _program)" and "vulProperty(_vulID, _range, _consequence)" to model vulnerabilities exhibited by nodes.

2. A node in N_c represents the predicate that codifies the post attack state as the consequence of an attack step. We use predicates "execCode(_host,_user)" and "netAccess(_machine,_protocol, _port)" to model the attacker's capability after the attack step. Valid instantiations of these predicates after an attack will update valid instantiation of the predicates listed in (1).

3. A node in N_r consists of a single rule of the form $p \Leftarrow p_1 \wedge p_2,.,\wedge p_n,$ where p as the child node of N_r is an instantiation of predicates from N_c, and all p_i for $i \in \{1,\ldots n\}$ as the parents nodes of N_r are the collection of all predicate instantiations of N_f from the current step and N_c from all prior attack steps.

Figure 1 is an example LEG (the notation of all nodes is in the Table 1), where fact, rule and consequence fact nodes are represented as boxes, ellipses, and diamonds respectively. Consequence fact nodes (Node 1 and 3) codify attack status obtainable from event logs or other forensic tools recording the post-conditions of attack steps. Facts (Node 5, 6, 7 and 8) include software vulnerability (Node 8) extracted from a forensic tool by analyzing captured evidence, computer configuration (Node 7) and network topology of a network (Node 5, 6). Rule nodes (node 4 and 2) represent specific rules that change the attack status based on attack steps. These rules have to be created from expert knowledge and are used to link chains of evidence as consequences of attack steps. Linking the chain of evidence using a rule forms an investigator's hypothesis of an attack step given the evidence.

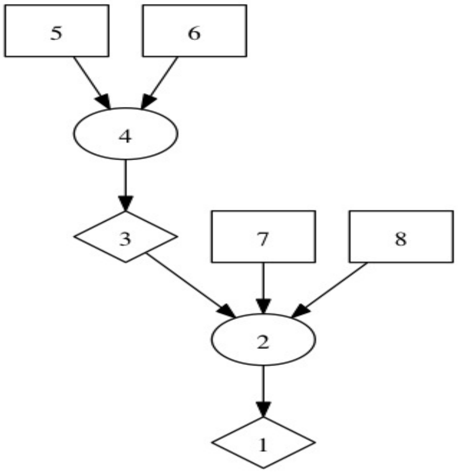


Figure 1: An Example Logical Evidence Graph

Table 1: The notation of nodes in Figure 1

Node	Notation	Resource
1	execCode(workStation1,user)	Evidence obtained from event log
2	THROUGH 3 (remote exploit of a server program)	Rule 1 (hypothesis 1)
3	netAccess(workStation1,tcp,4040)	Evidence obtained from event log
4	THROUGH 8 (direct network access)	Rule 2 (hypothesis 2)
5	hacl(internet,workStation1,tcp,4040)	Network Setup
6	attackerLocated(internet)	Fact
7	networkServiceInfo(workStation1,httpd,tcp,4040,user)	Computer Setup
8	vulExists(workStation1,'CVE-2009-1918', httpd,remoteExploit,privEscalation)	Vulnerability obtained from IDS Alert

Figure 2 lists the two rules, Rule 1 and Rule 2 in Table 1, between Line 9 and Line 17. Rules use the Prolog notation ": -" to separate the head (consequence) and the body (facts). In

Figure 2, Line 1 to Line 8 identifies fact and consequence predicates of the two rules. Rule 1 between Line 9 to Line 12 in Figure 2 represents an attack step that states: if (1) the attacker is located in a “Zone” such as internet (Line 10- attackerLocated(Zone)), and (2) if a host computer “H” can be accessed from the “Zone” by using “Protocol” at “Port”(Line 11-hacl(Zone, H, Protocol, Port)), then (3) the host “H” can be accessed from the “Zone” by using “Protocol” at “Port” (Line 9- netAccess(H, Protocol, Port)) by using (4) “direct network access” (Line 12--the description of the rule). Rule 2 between Line 13 to 17 states: (1) if a host has software vulnerability that can be remotely accessed (Line 14- vulExists(H, _, Software, remoteExploit, privEscalation), (2) the host can be reached by using “Protocol” at “Port” with privilege “Perm” (Line 15- networkServiceInfo(H, Software, Protocol, Port, Perm)), and (3) the attacker can access host by “Protocol” and “Port” (Line 16-netAccess(H, Protocol, Port)), then the attacker can remotely exploit the host “H” and obtain the privilege “Perm”(Line 13- execCode(H, Perm)) by using “'remote exploit of a server program” technique (Line 17).

```
//Rule Head--post attack status as derived fact obtained from forensic analysis on evidence
1. Consequence:  execCode(_host, _user).
2. Consequence: netAccess(_machine,_protocol,_port).

// Rule body--access priviledge
3. Fact:  hacl(_src, _dst, _prot, _port).

 //Rule body--software vulnerability obtained from forensic tool
4. Fact: vulExists(_host, _vulID, _program).
5. Fact: vulProperty(_vulID, _range, _consequence).

//Rule body--network topology
6. Fact: hacl(_src, _dst, _prot, _port).
7. Fact: attackerLocated(_host).

//Rule body--computer configuration
8. Fact: hasAccount(_principal, _host, _account).

 Rule 1:
9.  (netAccess(H, Protocol, Port) :-
        attackerLocated(Zone),
        hacl(Zone, H, Protocol, Port)),
        rule_desc('direct network access', 1.0).

Rule 2:
(execCode(H, Perm) :-
        vulExists(H, _, Software, remoteExploit, privEscalation),
        networkServiceInfo(H, Software, Protocol, Port, Perm),
       netAccess(H, Protocol, Port)),
       rule_desc('remote exploit of a server program', 1.0).
```

Figure 2: The Example Rules Representing Attack Techniques

4. COMPUTING PROBABILITIES USING BAYESIAN INFERENCE

Bayesian networks [3] are an efficient graphical representation scheme, where the nodes of a directed acyclic graph (DAG) represent random variables (RVs), events or evidence, and arcs model direct dependencies between RVs, events or evidence. Every node has a table (CPT) that provides the conditional probability of the node’s variable given the combination of its parent variables’ states.

Definition 2 (Bayesian Network): Suppose random variables $X_1,X_2,...,X_n$ are n random variables connected in a DAG, the joint probability distribution of $X_1,X_2,...,X_n$ can be computed by using the Bayesian formula $P(X_1,X_2,\ldots,X_n) = \prod_{j=1}^{n} [\![P(X_j) | Parent(X_j)]\!]$, in which $parent(X_j)= \{X_i \mid arc\ (i \rightarrow j) \text{ is in the graph}\}$.

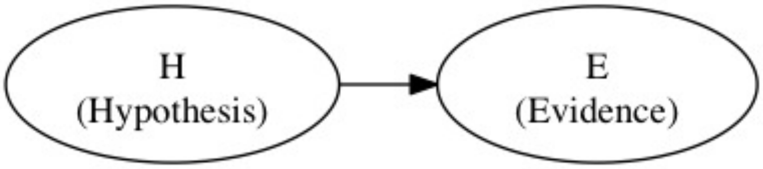


Figure 3: Causal View of Evidence

A BN can model and visualize dependencies between the hypothesis and evidence to calculate the revised probability when any evidence is presented [11]. Dependency probability of a hypothesis H about created scenarios on discovered evidence E can be modeled as shown in

Figure 3. Hence, Bayes' theorem can be used to update an investigator's belief about a hypothesis H when the evidence E is observed, using Equation (1):

$$\mathrm{P(H|E)}=\frac{P(H)P(E|H)}{P(E)}=\frac{P(H)P(E|H)}{\mathrm{P(E|H)*P(H)+P(E|no\ \ H)*P(no\ \ H)}} \qquad (1)$$

In Equation (1), P(H|E) is the posterior probability of an investigators' belief on hypothesis H given the evidence E. P(E|H) needs to come from experts' knowledge, which is referred to as the likelihood function that assesses the probability of evidence assuming the truth of H. P(H) is the prior probability of H when the evidence has not been discovered, and P(E) = P(E|H)*P(H) + P(E| not H)*P(not H) is the probability of the evidence irrespective of the experts' knowledge about H, which is referred to as a normalizing constant [1,7].

4.1 Calculating P(H|E) in a Logical Evidence Graph

An LEG is consists of a serial application of attack steps, which can be mapped to a Bayesian network as follows: (1) "N_c" as the child of the corresponding "N_r" shows that an attack step happened; (2) "N_r" is the hypothesis on the attack step, denoted by "H"; (3) "N_f" from the current attack step and "N_c' " from last attack step as the parents of "N_r" are attack evidence, showing the exploited vulnerability and the attack privilege the attacker used to launch the attack step; (4) the current "N_c" (also used as the pre-condition of next attack step) propagates the dependency between the current attack step and the subsequent one.

4.1.1. Computing P(H|E) for a Consequence Fact Node

Equation (1) can be used to compute P(H|E) for a consequence fact node of a single attack step when the prior attack step has not been considered, where the rule node provides the hypothesis H, both the fact node "N_f" and the consequence node from a prior attack step "N_c'" provide evidence E. Because a hypothesis H is a rule node "N_r", Bayes' theorem implies Equation (2):

$$\mathrm{P(H|E)=P(N_r|E)}=\frac{P(\mathrm{Nr})P(\mathrm{E|Nr})}{P(\mathrm{E})} \qquad (2)$$

The fact nodes from current attack step and consequence fact node from a prior attack step are independent to each other. They provide the body of the rule, deriving the consequence fact node for current attack step as the head of the rule. Consequently, their logical conjunction provides the conditions that are used to arrive at the conclusion of rule. Accordingly, if a rule node has k many parents N_{p1}, N_{p2}, …, N_{pk} that are independent, $P(E)= P(N_{p1},N_{p2},\ldots,N_{pk}) = P(N_{p1}\cap N_{p2}\cap\ldots\cap N_{pk})=P(N_{p1}).P(N_{p2})\ldots.P(N_{pk})$. Due to independence, given the rule N_r, $P(E|N_r)= P(N_{p1}, N_{p2},.., N_{pk}|N_r)=P(N_{p1}|N_r).P(N_{p2}|N_r)\ldots P(N_{pk}|N_r)$. Hence, by applying Equation (2) where H is N_r and E is $N_{p1}\cap N_{p2}\cap\ldots\cap N_{pk}$, we get Equation (3) that we use to compute P(H|E) for a consequence fact node.

$$\mathrm{P(H|E)=P(N_r|\ N_{p1},N_{p2},\ldots,N_{pk})}=\frac{P(\mathrm{Nr})\mathrm{P(Np1\ |Nr).P(Np2\ |Nr)\ldots\ P(Npk\ |Nr)}}{P(\mathrm{Np1})P(\mathrm{Np2})\ldots P(\mathrm{Npk})} \qquad (3)$$

However, because $P(E|N_r)$ is a forensic investigators' subjective judgment, the investigator may directly assign $P(E|N_r)$ instead of assigning $P(N_{p1}|N_r)$, $P(N_{p2}|N_r)$ … $P(N_{pk}|N_r)$ separately. We allow the investigators' discretion of using Equations (2) or (3).

4.1.2. Computing P(H|E) for the Entire Logical Evidence Graph

Now we show how to compute P(H|E) for the whole evidence graph composing of attack paths. Any chosen attack path in a LEG consists of a serial application of attack steps. Suppose S_i（i＝1 to n) represents the i^{th} attack step in such a path. From the equation in Definition (2), we get Equation (4) as follows, where any attack step only depends on its direct parent attack step, but is independent from all other ancestor attack steps in the attack path.

$$P(H|E) = P(H_1,H_2\ldots H_n|E_1,E_2,E_3\ldots E_n) = P(S_1)P(S_2|S_1)\ldots.P(S_n|S_{n-1}) \qquad (4)$$

Let $N_{i,f}$, $N_{i,r}$ and $N_{i,c}$ be the fact, rule and consequent fact node at the i-th attack step. Equation (4) can be written as Equation (5) as follows.

$$P(H|E) = P(S_1)P(S_2|S_1)\ldots.\ P(S_i|S_{i-1})\ldots\ P(S_n|S_{n-1})$$

$$= P(N_{1,r}|N_{1,f})\ P(N_{2,r}|\ N_{1,c},\ N_{2,p})\ \ldots\ P(N_{i,r}|\ N_{i-1,c},\ N_{i,p})\ \ldots\ P(N_{n,r}|\ N_{n-1,c},\ N_{n,p})$$

$$=\frac{P(\mathrm{N1,r})P(\mathrm{N1,f|N1,r})}{P(\mathrm{N1,f})}\ldots\frac{P(\mathrm{Ni,r})P(\mathrm{Ni-1,c,Ni,f|Ni,r})}{P(\mathrm{Ni-1,c,Ni,f})}\ldots\frac{P(\mathrm{Nn,r})P(\mathrm{Nn-1,c,Nn,f|Nn,r})}{P(\mathrm{Nn-1,c,Nn,f})} \qquad (5)$$

where "$P(S_1).P(S_2|S_1)\ldots.\ P(S_i|S_{i-1})$" is the joint posterior hypothesis of the prior i attack steps (including attack step 1, 2,… i) given all evidence from these attack steps (evidence for attack step 1 is $N_{1,f}$; evidence for attack step i includes $N_{i-1,c}$ and $N_{i,f}$ where i goes from 2 to n.). It is propagated to i+1-th attack step by the sequence fact node $N_{i,c}$ that is used as the pre-condition of the i+1-th attack step. Algorithm 1 presents this description in the algorithmic format.

ALGORITHM 1:

Input: A logical evidence graph LEG=(N_r,N_f,N_c,E,L,G) that may have multiple attack paths, and $P(N_{i,r})$(i=1 to n), $P(N_{1,f}|N_{1,r}|)$, $P(N_{1,f})$, $P(N_{i-1,c},N_{i,f}\ |N_{i,r})$,$P(N_{i-1,c},N_{i,f})$ (i=2 to n) from expert knowledge for each attack path($[N_{1,f}]$ and $[N_{i-1,c},N_{i,f}]$(i>=2) are evidence E. $P(N_{i,r})$(i>=1) is H).

Output: The joint posterior probability of the hypothesis of every attach path, $P(H|E)=P(H_1,H_2\ldots H_n|E_1,E_2,E_3\ldots E_n)$ (P(H|E) is written as P in the algorithm) , given all evidence represented by fact nodes $N_{i,f}$ and $N_{i,c}$(i=1 to n).

```
Begin
$Q_g \leftarrow Ø$          // set the $Q_g$ to empty
For each node n $\in$ LEG do
      color[n] $\leftarrow$ WHITE      // color every node in the graph to white
End
ENQUEUE($Q_g$, $N_{1,f}$)              // push all fact nodes from first attack steps to queue $Q_g$
j $\leftarrow$0                           // use j to record which attack path we are computing
While ($Q_g$ ≠     )                / when queue $Q_g$ is not empty
  Do n $\leftarrow$DEQUEUE($Q_g$ )       //take out a fact node n
         $N_{1,r} \leftarrow$ child[n]         //find a rule node as the child node of n
      If color[$N_{1,r}$] == WHITE   // if this rule node is not traversed (white)
         Then j $\leftarrow$ j+1                  // it must be a new attack path
              P[j] $\leftarrow$PATH($N_{1,r}$ )  // calculate joint posterior probability of the path
              color[$N_{1,r}$] $\leftarrow$BLACK  //mark this rule node as black
End
```

PATH($N_{1,r}$)   //calculate the posterior probability of an attack path

```
15.   $N_{1,c} \leftarrow$ child[$N_{1,r}$]          // the consequence fact node of first attack step
16.   E $\leftarrow$ parents [$N_{1,r}$]          // E is the evidence for the first attack step
17.   P[$N_{1,c}$] $\leftarrow \frac{P(\mathrm{N1,r})P(\mathrm{E}|\mathrm{N1,r})}{P(\mathrm{E})}$        // the probability for first attack step
18.   color[E] $\leftarrow$ BLACK               //mark all evidence to black color
19.   P$\leftarrow$P[$N_{1,c}$]                        // use P to do cursive computation
20.   For i $\leftarrow$ 2 to n do           // from the second attack step to the last attack step
21.       $N_{i,r} \leftarrow$child[$N_{i-1,c}$]    // the rule node as H of $i^{th}$ attack step
22.       E $\leftarrow$ parents[$N_{i,r}$]  //the evidence for the $i^{th}$ attack step
23.       $N_{i,c} \leftarrow$ child[$N_{i,r}$]    // the consequence fact node of $i^{th}$ attack step
          // the posterior possibility for the $i^{th}$ attack step
24.       P [$N_{i,c}$ ] $\leftarrow$P($N_{i,r}$| E) $\leftarrow \frac{P(\mathrm{Ni,r})P(\mathrm{E}|\mathrm{Ni,r})}{P(\mathrm{E})}$
25.       color[E] $\leftarrow$ BLACK  //mark all traversed evidence to black color
26.       P$\leftarrow$ P. P($N_{i,c}$)  // joint posterior possibility of attack steps of (1 … i)
27.   End
28.   Return P          //return the posterior attack possibility for this attack path
```

Algorithm 1: Computing P(H|E) for the entire Logical Evidence Graph

Because a logical evidence graph may have several attack paths, in order to compute each attack path's posterior probability, we color all nodes as white (Line 2, 3, 4), and push all fact nodes at the first attack step of all attack paths to an empty queue (Line 1, Line 5). When the queue is not empty (Line 7), we take a fact node out of the queue (Line 8), and decide if its child that is a rule node is white (Line 9 to 10). If the rule node is white, it gives a new attack path (Line 11), upon which we recursively use Equation (5) to compute the joint posterior probability for the entire attack path (the function is between Line 15 to Line 28) and color the node BLACK (Line 13) after the computation performed in function "PATH($N_{1,r}$)" (Line 12). We keep repeating the above process until the queue holding the fact nodes from first attack steps of all attack paths is empty.

4.2. Calculating the Cumulative False Positive of an Evidence Graph

As in any statistical estimation, false positives and false negatives exist in LEGs. A false negative arises in a step when an investigator believes that the event was not caused by an attack, but was due to an attack. A false positive arises when an investigator believes that an event was caused by the chosen attack, but was not. Therefore, we wish to estimate both. Because the logical evidence graph is constructed by using attack evidence chosen by the forensic investigator, that creates the possibility of false positive evidence, we quantify the cumulative false positive rate of the constructed attack path so that the investigator can estimate the false positive rate of an entire attack path. We do not estimate false negatives in this paper.

The individual false positive estimate on an attack step is formalized as $P(E|\neg H)$, where $\neg H$ is the alternative hypothesis, usually written as "not H", and the value of $P(E|\neg H)$ can be computed from prior forensic data using statistics. In order to show how to compute the cumulative false positive rate of an entire attach path, we let our notation $N_{i,f}$, $N_{i,r}$ and $N_{i,c}$ be the fact, rule and consequence fact node of the i^{th} attack stack step. Then, the cumulative false positive rate of an entire attack path can be computed as follows (Notice that all evidence supporting an attack step is independent from evidence supporting other attack steps).

$$\begin{aligned} P(E|\neg H) &= P(E_1,E_2,\dots,E_n|\neg(H_1,H_2\dots H_n)) \\ &= P(E_n|\neg N_{n,r})\cup P(E_1,E_2,\dots ,E_{n-1} |\neg N_{n-1,r}) \\ &=\dots\dots \\ &= P(E_n|\neg N_{n,r}) \cup P(E_{n-1}|\neg N_{n-1,r}) \cup\dots\cup P(E_1|\neg N_{1,r}) \\ &= P(E_1|\neg N_{1,r}) \cup \dots\cup P(E_{n-1}|\neg N_{n-1,r}) \cup P(E_n|\neg N_{n,r}) \\ &=1-(\dots\dots (1-(1- P(E_2|\neg N_{2,r}) .(1- P(E_1|\neg N_{1,r}))).(1- P(E_n|\neg N_{n,r})) \end{aligned} \quad (6)$$

As described earlier, in Equation (6), E_1 is $N_{1,f}$, and E_i includes $N_{i-1,c}$ and $N_{i,f}$(i= 2 to n). The union symbol"$\cup$" represents the disjunction "or", which is observed to be equivalent to the noisy-OR operator [9]. For a serial connection, if any of the attack steps is a false positive, the whole attack path is considered false positive. Algorithm 2 presents the computation of $P(E|\neg H)$ for the entire evidence graph in the algorithmic form.

ALGORITHM 2:

Input: A logical evidence graph $LEG=(N_r,N_f,N_c,E,L,G)$, and $P(N_{1,f}|N_{1,r})$ as $P(E_1|H_1)$, $P(N_{i-1,c},N_{i,f}|N_{i,r})$ as $P(E_i|H_i)$(i=2 to n) for every attack path.

Output: The cumulative false positive rate of each attach path $P(E|\neg H)= P(E_1,E_2,\ldots,E_n|\neg(H_1,H_2\ldots H_n))$(written as P_f).

```
Begin
1. $Q_g \leftarrow \emptyset$          // set the $Q_g$ to empty
2. For each node $n \in$ LEG do
3.         color[n] $\leftarrow$ WHITE      // color every node in the graph to white
4. End
5. ENQUEUE($Q_g$, $N_{1,f}$)              // push all fact nodes from first attack steps to queue $Q_g$
6. j $\leftarrow$ 0                              //  use j to record which attack path we are computing
7. While ($Q_g \neq$     )              // when queue $Q_g$ is not empty
8.    Do   $\leftarrow$DEQUEUE($Q_g$)      //take out a fact node n
9.              $N_{1,r} \leftarrow$ child[n]         //find a rule node as the child node of n
10.             If color[$N_{1,r}$] == WHITE   // if this rule node is not traversed (white)
11.               Then  j$\leftarrow$ j+1                // it must be a new attack path
12.                       $P_r$[j] $\leftarrow$PATH($N_{1,r}$ )  // calculate cumulative false positive rate of the path
13.                       color[$N_{1,r}$] $\leftarrow$BLACK  //mark this rule node as black
14. End

PATH($N_{1,r}$)       //calculate the cumulative false positive rate of an attack path
15.  $N_{1,c} \leftarrow$ child[$N_{1,r}$]          // the consequence fact node of first attack step
16.  E $\leftarrow$ parents[$N_{1,r}$]           // E is the evidence for the first attack step
17.  P[$N_{1,c}$]$\leftarrow$ $P(E|\neg N_{1,r})$        // the false positive rate of the first attack step
18.  color[E] $\leftarrow$ BLACK  //mark all traversed evidence to black color
19.  $P_f \leftarrow$ P[$N_{1,c}$]             //use $P_f$  to do recursive computation below
20.  For i $\leftarrow$ 2 to n do    // from attack step 2 to attack step n
21.        $N_{i,r}\leftarrow$child[$N_{i-1,c}$]    // the rule node of $i^{th}$ attack step
22.        $N_{i,c} \leftarrow$ child[$N_{i,r}$]    // the consequence fact node of $i^{th}$ attack step
23.        E $\leftarrow$ parents[$N_{i,r}$]   //the evidence for the $i^{th}$ attack step
24.        $P_f \leftarrow 1-(1- P_f).(1- P(E|\neg N_{i,r}))$  //the cumulative false positive rate
25.        color[E] $\leftarrow$ BLACK  // mark all traversed evidence to black color
26.  End
27.  Return $P_f$      // return the cumulative false positive rate of the attack path
```

Algorithm 2: Computing $P(E|\neg H)$ for the Entire Evidence Graph

In Algorithm 2, Line 1 to Line 14 are the same as Algorithm 1, which is used to find a new attack path. Line 15 to Line 27 use Equation (6) to recursively compute cumulative false positive rate for an entire attack path.

5. CASE STUDY

In this Section, we show how to reconstruct probabilistic attack scenarios by building Bayesian Network analysis into our Prolog-based reasoning tool [4].

5.1 **The Experimental Network**

Figure 4 shows an experimental network from [4], which we used as a case study to show how to generate a logical evidence graph from post-attack evidence. In this network, the external Firewall 1 controls network access from the Internet to the network, where a webserver hosts two web services—Portal web service and product web service. The internal Firewall 2 controls the access to a SQL database server that can be accessed from webservers and workstations. The administrator has administrative privilege on the Portal webserver that has a forum for users to chat with the administrator. We used SNORT as the IDS and configured both web servers and the database server to log all accesses and queries as events. We use them as attack evidence.

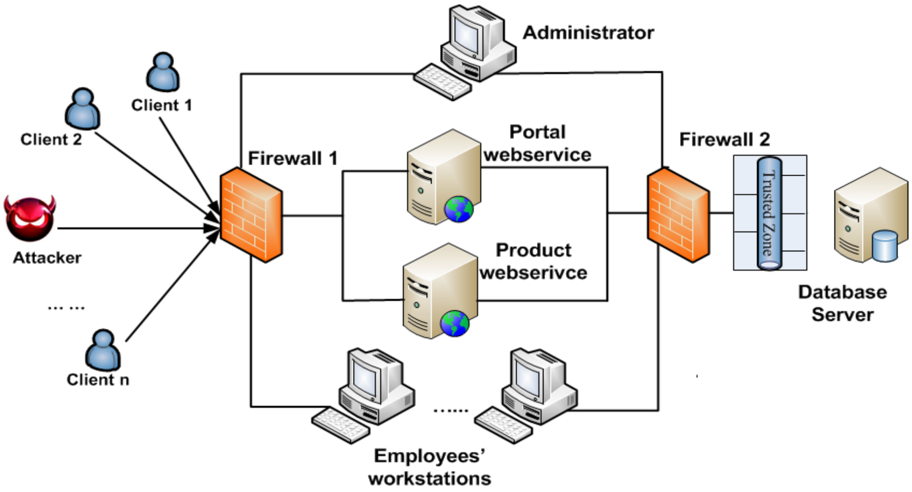


Figure 4: An Experimental Attack Network

By exploiting vulnerabilities in a Windows workstation and a web server that have access to the database server, we, who simulated the attacker, were able to successfully launch two kinds of attacks on the database server and a Cross Site Scripting (XSS) attack towards the administrator's computer. These attacks include (1) using a compromised workstation to access the database server (CVE-2009-1918), (2) exploiting the vulnerability on the web server application (CWE89) to attack the database server， and (3) exploiting XSS vulnerability on the chat forum hosted by the portal web service to steal the administrator's session ID, which allowed the attacker to send out phishing emails to the clients, tricking them to update their confidential information.

Our IDS and the logging system in the network detected some attack activities. We pre-processed them to data as shown in Table 2. The post attack status obtained by using forensic tools is also formalized to Table 3.

Table 2: Formalized Evidence of the Alerts and Log from Figure 4

Timestamp	Source IP	Destination IP	Content/Observed Events	Vulnerability
08/13-12:26:10	129.174.124.122 Attacker	129.174.124.184 Workstation1	SHELLCODE x86 inc ebx NOOP	CVE-2009-1918
08/13-12:27:37	129.174.124.122 Attacker	129.174.124.185 Workstation2	SHELLCODE x86 inc ebx NOOP	CVE-2009-1918
08/13-14:37:27	129.174.124.122 Attacker	129.174.124.53 Product Web Server	SQL Injection Attempt	CWE89
08/13-16:19:56	129.174.124.122 Attacker	129.174.124.137 Administrator	Cross Site Scripting	XSS
08/13-14:37:29	129.174.124.53 Product Web Server	129.174.124.35 Database Server	name='Alice' AND password='alice' or '1'='1'	CWE89
…				

Table 3: Post Attack Status from Attacks in Figure 4

Timestamp	Attacked Computer	Attack Event	Post Attack Status
08/13-14:37:29	129.174.124.35 Database Server	Information retrieved maliciously	Malicious Access
… …			

5.2 Constructing the Logical Evidence Graph

To use our Prolog-based rules for evidence graph construction, we codified evidence and system state to instantiations of predicates used in these rules as listed in Figure 5, where Lines 1, 2, 3 model evidence representing post attack status (Table 3); Lines 4 to 10 model network topology (system setup); Line 11 to 14 model system configurations and Lines 15 to 21 mode vulnerabilities obtained from captured evidence (Table 2).

```
//Observed Attack Events
1. attackGoal(execCode(workStation1,_)).
2. attackGoal(execCode(dbServer,user)).
3. attackGoal(execCode(clients,user)).

//Network Topology
4. attackerLocated(internet).
5. hacl(internet, webServer, tcp, 80).
6. hacl(internet, workStation1,tcp,_).
7. hacl(webServer, dbServer,tcp,3660).
8. hacl(internet,admin,_,_).
9. hacl(admin,clients,_,_).
10. hacl(workStation1,dbServer,_,_).

//Computer Configuration
11. hasAccount(employee, workStation1, user).
12. networkServiceInfo(webServer , httpd, tcp , 80 , user).
13. networkServiceInfo(dbServer , httpd, tcp , 3660 , user).
14. networkServiceInfo(workStation1 , httpd, tcp , 4040 , user).

/* Information From Table 1---software vulnearbility */
15. vulExists(webServer, 'CWE89', httpd).
16. vulProperty('CWE89', remoteExploit, privEscalation).

17. vulExists(dbServer, 'CWE89', httpd).
18. vulProperty('CWE89', remoteExploit, privEscalation).

19. vulExists(workStation1, 'CVE-2009-1918', httpd).
20. vulProperty('CVE-2009-1918', remoteExploit, privEscalation).
21.  timeOrder(webServer,dbServer,14.3727,14.3729).
…
```

Figure 5: The Input File for Logical Evidence Graph Generation

We ran the input file on rules that represent generic attack techniques in our reasoning system with two databases, an anti-forensic and MITRE's OVAL [2], to remove irrelevant evidence and find explanations for missing evidence. They are: (1) According to MITRE OVAL database, the "Workstation 2" is a Linux machine that uses Firefox as the web browser, which does not support a successful attack by using "CVE-2009-1918" that only succeeds on Windows Internet Explorer; (2) a new attack path representing that the attacker launched a phishing attack towards the clients by using the compromised administrators session ID has been found; (3) an attack path between the compromised workstation1 and the database server has been found.

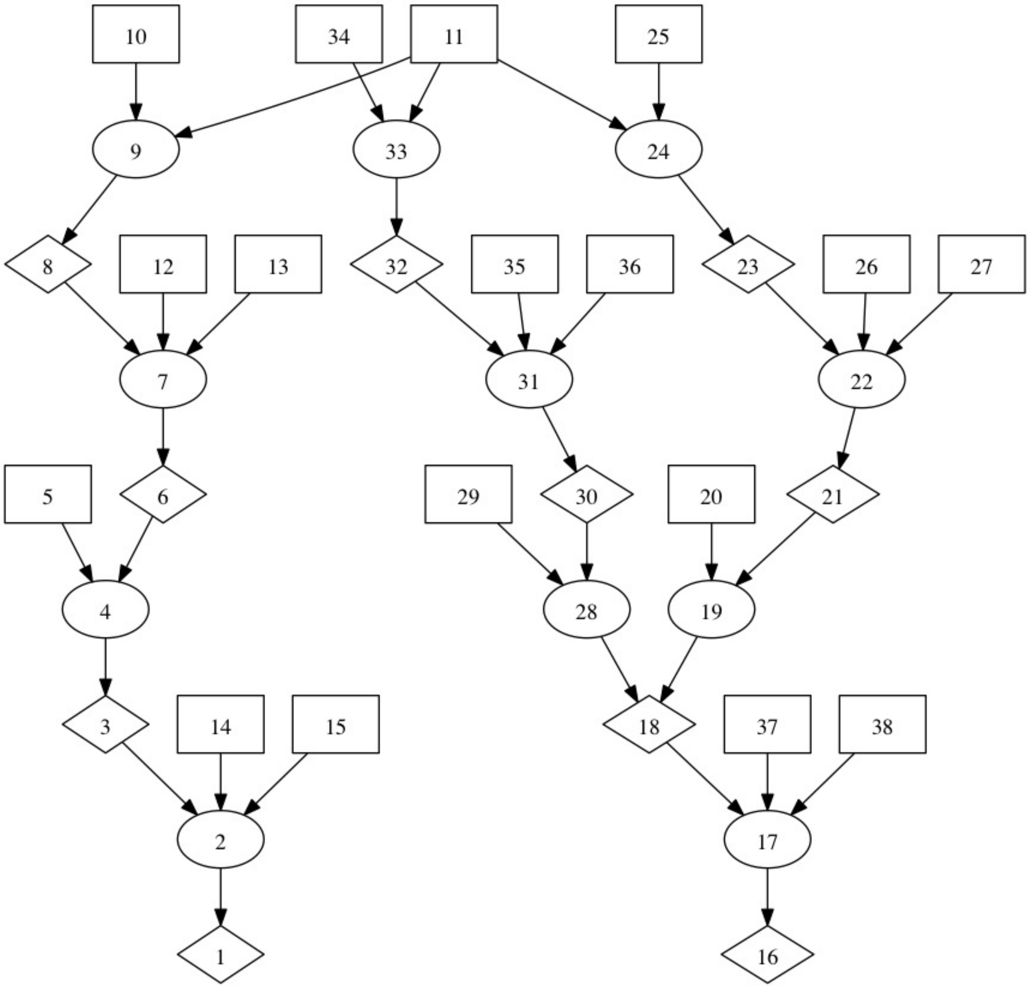


Figure 6: the Constructed Evidence Graph

The output of our tool created the logical evidence graphs shown in Figure 6. In order to limit the graph size, the notation of nodes in Figure 6 is shown in Column 2 in Table 4. In the same table, Column 3 is the logic operators used to distinguish fact nodes, rule nodes and consequence fact nodes, where all fact nodes are marked as “LEAF”; all rule nodes are marked as “OR”; and all consequence nodes are marked as “AND”. There are three attack paths in Figure 6, which are: (1) the attacker used a XSS attack to steal the administrator’s session ID and therefore obtain the administrator’s privilege to send out phishing emails to clients (11→ 9 → 8 → 7 → 6→ 4→ 3→ 2→ 1)(left); (2) the attacker used a buffer overflow vulnerability (CVE-2009-1918) to compromise the workstation, then obtained access to the database

(34→33→32→31→30→28→18→17→16) (Middle); and (3) the attacker used a web application that does not sanitize users' input (CWE89) to launch a SQL injection attack toward the database (11→24→23→22→21→19→18→17→16) (right).

Table 4: the Notation of Nodes in Figure 6

Node	Notation	Relation
1	execCode(clients,user)	OR
2	THROUGH 3 (remote exploit of a server program)	AND
3	netAccess(clients,tcp,_)	OR
4	THROUGH 7 (multi-hop access)	AND
5	hacl(admin,clients,tcp,_)	LEAF
6	execCode(admin,apache)	OR
7	THROUGH 3 (remote exploit of a server program)	AND
8	netAccess(admin,tcp,80)	OR
9	THROUGH 8 (direct network access)	AND
10	hacl(internet,admin,tcp,80)	LEAF
11	attackerLocated(internet)	LEAF
12	networkServiceInfo(admin,httpd,tcp,80,apache)	LEAF
13	vulExists(admin,'XSS',httpd,remoteExploit,privEscalation)	LEAF
14	networkServiceInfo(clients,httpd,tcp,_,user)	LEAF
15	vulExists(clients,'Phishing',httpd,remoteExploit,privEscalation)	LEAF
16	execCode(dbServer,user)	OR
17	THROUGH 3 (remote exploit of a server program)	AND
18	netAccess(dbServer,tcp,3660)	OR
19	THROUGH 7 (multi-hop access)	AND
20	hacl(webServer,dbServer,tcp,3660)	LEAF
21	execCode(webServer,user)	OR
22	THROUGH 3 (remote exploit of a server program)	AND
23	netAccess(webServer,tcp,80)	OR
24	THROUGH 8 (direct network access)	AND
25	hacl(internet,webServer,tcp,80)	LEAF
26	networkServiceInfo(webServer,httpd,tcp,80,user)	LEAF
27	vulExists(webServer,'CWE89',httpd,remoteExploit,	LEAF
28	THROUGH 7 (multi-hop access)	AND
29	hacl(workStation1,dbServer,tcp,3660)	LEAF
30	execCode(workStation1,user)	OR
31	THROUGH 3 (remote exploit of a server program)	AND
32	netAccess(workStation1,tcp,4040)	OR
33	THROUGH 8 (direct network access)	AND
34	hacl(internet,workStation1,tcp,4040)	LEAF
35	networkServiceInfo(workStation1,httpd,tcp,4040,user)	LEAF
36	vulExists(workStation1,'CVE-2009-1918',httpd,remoteExploit,privEscalation)	LEAF
37	networkServiceInfo(dbServer,httpd,tcp,3660,user)	LEAF
38	vulExists(dbServer,'CWE89',httpd,remoteExploit,privEscalation)	LEAF

5.3 Calculate Conditional Posterior Probabilities and False Positives

In this Section, we use Algorithm 1 and Algorithm 2 to calculate $P(H|E_1,E_2..E_n)$ and $P(E_1,E_2..E_n\ |\neg H)$ for attack paths in Figure 6.

5.3.1 Using Algorithm 1 to Calculate $P(H|E_1,E_2..E_n)$

Algorithm 1 requires [$P(N_{1,r})$, $P(N_{1,f}\ )$, $P(N_{1,f}\ |\ N_{1,r})$], [$P(N_{i,r})$, $P(N_{i\text{-}1,c}, N_{i,f}|\ N_{i,r})$, $P(N_{i\text{-}1,c}\ , N_{i,f})$ (i>1)]. All these probabilities are obtained from expert knowledge. To minimize the subjectivity of the impact, we suggest using the average number from many forensic experts' judgments [7]. Because the case study mainly focuses on how to do the computation, for simplicity, we let all $P(H_i) = P(\neg H_i) = 50\%$, $P(E_i) = k$(k is between 0 and 1. In real scenario, "k" differs for different evidence.), and assigned $P(E_i|H_i)$ from our judgments on those attack steps as shown in Table 5. Thus, the $P(H_i|E_i)$ for every attack step without considering about other attack steps is $\frac{P(\mathrm{Hi})P(\mathrm{Ei|Hi})}{P(\mathrm{Ei})}$= $\frac{0.5.P(\mathrm{Ei|Hi})}{k}$ $=$ $\frac{P(\mathrm{Ei|Hi})}{2k}$=c.$P(E_i|H_i)$ (let c=1/(2k)). By using Algorithm 1, we obtained $P(H|E_1,E_2..E_n)$ as shown in the last column of Table 5.

Table 5: Use Algorithm 1 to Compute $P(H|_{E1}\ldots E_n)$ for Attack Paths in Figure 6

Attack Path	**Attack Step 1**				**Attack Step 2**			
	H1	**P(E1|H1)**	**P(H1|E1)**	**P(H|E1)**	**H2**	**P(E2|H2)**	**P(H2|E2)**	**P(H|E1,E2)**
Left	Node 9	0.9	0.9c	0.9c	Node 7	0.8	0.8c	0.72c^2
Middle	Node 33	0.99	0.99c	0.99c	Node 31	0.87	0.87c	0.861c^2
Right	Node 24	0.99	0.99c	0.99c	Node 22	0.85	0.85c	0.842c^2
Attack Path	**Attack Step 3**				**Attack Step 4**			
	H3	**P(E3|H3)**	**P(H3|E3)**	**P(H|E1,E2,E3)**	**H4**	**P(E4|H4)**	**P(H4|E4)**	**P(H|E1,E2,E3,E4)**
Left	Node 4	0.9	0.9c	0.648c^3	Node 2	0.75	0.75c	0.486c^4
Middle	Node 28	0.87	0.87c	0.75c^3	Node 17	0.75	0.75c	0.563c^4
Right	Node 19	0.97	0.97c	0.817c^3	Node 17	0.95	0.95c	0.776c^4

Notice Node 17 has two joint posterior conditional probabilities, which are from middle path and right path respectively. We can notice that the attack path from the former has smaller probability than the latter. That is because the evidence from middle path that involves using a compromised workstation to get access to the databases was hard to be found. Correspondingly, the $P(E_i|H_i)$ is smaller. Therefore, the corresponding hypothesized attack path has a much smaller probability $P(H|E_1,E_2..E_n)$(H is $H_1 \cap \ldots H_n$). In reality, it is almost impossible for the same attacker to try a different attack path to attack the same target if he already succeeded. A possible scenario would be that if the first attack path did not succeeded, the attacker would try the second attack path to launch the attack. The joint posterior conditional probability $P(H|E_1,E_2..E_n)$ could help investigator to judge which attack path is the one that is most possibly used.

5.3.2 Using Algorithm 2 to Calculate $P(E_1,E_2..E_n |\neg H)$

Algorithm 2 requires $P(N_{1,f}|N_{1,r})$ as $P(E_1|\neg H_1)$, $P(N_{i-1,c},N_{i,f} |N_{i,r})$ as $P(E_i|\neg H_i)$(i=2 to n) to recursively compute $P(E_1,E_2..E_n |\neg H)$ (H is $H_1 \cap \ldots H_n$). As an example, we assigned $P(E_i|\neg H_i)$ for different attack step in the three attack paths in Table 6 and calculated $P(E_1,E_2..E_n |\neg H)$, showing that the right attack path has the smallest cumulative false positive estimate.

Table 6: Use Algorithm 2 to Calculate $P(E_1,E_2..E_n |\neg H)$

Attack Path	**Attack Step 1**			**Attack Step2**		
	H_1	**$P(E_1 \mid \neg H_1)$**	**$P(E_1 \mid \neg H_1)$**	**H_2**	**$P(E_2 \mid \neg H_2)$**	**$P(E_1,E_2 \mid \neg H)$**
Left	Node 9	0.002	0.002	Node 7	0.001	0.003
Middle	Node 33	0.002	0.002	Node 31	0.003	0.005
Right	Node 24	0.002	0.002	Node 22	0.001	0.003
Attack path	**Attack Step3**			**Attack Step4**		
	H_3	**$P(E_3 \mid \neg H_3)$**	**$P(E_1,E_2,E_3 \mid \neg H)$**	**H**	**$P(E_4 \mid \neg H_4)$**	**$P(E_1,E_2,E_3,E_4 \mid \neg H)$**
Left	Node 4	0.004	0.007	Node 2	0.03	0.0368
Middle	Node 28	0.003	0.008	Node 17	0.04	0.0477
Right	Node 19	0.002	0.005	Node 17	0.007	0.012

Values computed for $P(H|E_1,E_2..E_n)$ and $P(E_1,E_2..E_n |\neg H)$ show that the right attack path (11→24→23→22→21→19→18→17→16) is a better attack path to be chosen by an investigator because it has the largest $P(H|E)$ and smallest $P(E|\neg H)$; the left path is not convincing, because its joint posterior probability is less than 0.5c^4; and the middle path has a bigger cumulative false positive rate, in which the evidence should be re-evaluated to see if the attack path reflects the real attack scenario.

6. CONCLUSION

In this paper, we have described a method that uses rules to construct a logical evidence graph and maps it to a Bayesian Network so that the joint likelihood or false positive rate for the constructed attach paths could be computed automatically. By using a case study, we showed how our method could guide forensic investigators to choose the most likely attack scenarios that fit the available evidence. Our case study showed that our methodology and the accompany tool could be useful for network forensics investigation and analysis.

DISCLAIMER

This paper is not subject to copyright in the United States. Commercial products are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the identified products are necessarily the best available for the purpose.

REFERENCES:

[1] Bruno Olshausen, “Bayesian probability theory” March 1, 2004.

[2] https://oval.mitre.org/.

[3] Pearl, J. (1986). Fusion, propagation and structuring in belief networks. Artificial Intelligence, 29, 241-288.

[4] C. Liu, A. Singhal, D. Wijesekera: A Logic Based Network Forensics Model for Evidence Analysis. IFIP Int. Conf. Digital Forensics 2015.

[5] A. Darwiche, Modeling and Reasoning with Bayesian Networks, Cambridge University Press, April 06, 2009.

[6] F. Taroni, A. Biedermann, P. Garbolino, C.G. Aitken, A general approach to Bayesian networks for the interpretation of evidence Forensic Sci. Int., 139 (2004), pp. 5–16.

[7] M Kwan, K P Chow, F Law and P Lai. Reasoning About Evidence using Bayesian Network, Advances in Digital Forensics IV, International Federation for Information Processing (IFIP) January 2008, Tokyo, pp.141-155.

[8] B. Carrier, A Hypothesis-Based Approach to Digital Forensic Investigations (Ph.D. Thesis), 2006,West Lafayette: Purdue University.

[9] Y. Liu and H. Man, Network vulnerability assessment using Bayesian Networks, In Proceedings of SPIE - Data Mining, Intrusion Detection, Information Assurance and Data Networks Security (SPIE'05), pages 61–71, 2005.

[10] C. Vlek, H. Prakken, S. Renooij and B. Verheij(2013), Modeling crime scenarios in a Bayesian Network, the 14th International Conference on Artificial Intelligence and Law (ICAIL 2013), Proceedings of the Conference, 150–159, ACM Press, New York.

[11] Fenton, N.*,* Neil, M.*, &* Lagnado, D.A. *(*2012*),* A general structure for legal arguments about evidence using Bayesian networks*,* Cognitive Science*,* 37*,* 61–102.

[12] F. Taroni, S. Bozza, A. Biedermann, G. Garbolino, C.G.G. Aitken, Data Analysis in Forensic Science: A Bayesian Decision Perspective, John Wiley & Sons, Chichester (2010).

[13] X Ou, W. F. Boyer, M. A. McQueen, "A scalable approach to attack graph generation," In: 13th ACM Conference on Computer and Communications Security (CCS), pp. 336–345 (2006).

[14] MulVAL: A logic-based enterprise network security analyzer, retrieved from http://www.arguslab.org/mulval.html.

A Simulation Framework for Industrial Wireless Networks and Process Control Systems

Yongkang Liu, Richard Candell, *Senior Member, IEEE,* Kang Lee, *Fellow, IEEE,* and Nader Moayeri, *Senior Member, IEEE*

***Abstract*—Factory and process automation systems are increasingly employing information and communications technologies to facilitate data sharing and analysis in integrated control operations. Wireless connections provide flexible access to a variety of field instruments and reduce network installation and maintenance costs. This serves as an incentive for the adoption of industrial wireless networks based on standards such as the WirelessHART and ISA100.11a in factory control systems. However, process control systems vary greatly and have diverse wireless networking requirements in different applications. These requirements include deterministic transmissions in the shared wireless bandwidth, low-cost operation, long-term durability, and high reliability in the harsh radio propagation environment. It is an open question whether a generic wireless technology would meet the requirements of industrial process control. In this paper, we propose a novel simulation framework for performance evaluation of wireless networks in factory and process automation systems. We select a typical process control plant model, specifically the Tennessee Eastman Challenge (TE) Model, and define the interfaces between the process simulator and the wireless network simulator. We develop a model of the protocol stack of the WirelessHART specification in the OMNET++ simulation engine as a typical industrial wireless network. We present simulation results that validate the prospect of using WirelessHART in the TE plant, and we evaluate the impact of various wireless network configurations on the plant operation. Given its modular design, the proposed simulation framework can be easily used to evaluate the performance of other industrial wireless networks in conjunction with a variety of process control systems.**

***Index Terms*—industrial wireless networks, sensor networks, factory and process automation networks, WirelessHART, network simulation.**

I. Introduction

Cyber-physical systems (CPS) represent a paradigm shift that enables co-design of physical systems and advanced information and communications technology components to improve the effectiveness of physical systems through exchange, in-depth understanding, and exploitation of the data generated in the operations [1]. The process control and automation industry is one of the prominent application domains for CPS to improve production efficiency and eliminate potential risks and safety issues in plant operations [2]. An industrial process usually requires continuous status monitoring and timely response to any deviation from setpoints and key performance metrics. Therefore, a large number of sensors and actuators are employed by the process controller for control purposes. How to network these field instruments efficiently for process measurement and manipulation in the control system is still an ongoing research topic [3].

Wired connections are effective in supporting reliable, point-to-point communications between the controller and the field instruments. Hence, they were adopted early for process control communications, as exemplified by the HART standard [4]. However, wired connections cannot accommodate the growing demands for support of adaptive network topology and fast reconfiguration encountered in many process control systems. Instead of having to lay down miles of cables to connect hundreds of field instruments, industrial wireless communication networks provide wireless connections with customized network topology, enable plug-and-play configuration, and lower installation and maintenance costs [5]. Recently, many new industrial wireless protocols and mechanisms, such as WirelessHART [6] and ISA100.11a [7], have been proposed.

The study of industrial wireless networks is still in its infancy. Compared with Internet data services, process control operations have more rigid quality of service (QoS) requirements, including tighter message latency, lower power consumption, highly reliable transmissions in usage scenarios involving mobility and centralized data analytics [8]. As process control performance and network performance are closely coupled, a common evaluation framework for joint system design is essential and still missing. Although there exists a large and rich body of literature on control theory [9] and wireless networking [10], resulting from decades of research and development, a joint performance analysis of a system comprised of both components turns out to be difficult. On the other hand, simulation has proven to be a practical and economic approach to study the behavior of complex systems and evaluate competing solutions before field deployment [11]. The simulation-based approach has been adopted in several CPS studies dealing with smart grid systems [12] and vehicular ad hoc networks [13]. However, there is still a lack of a good simulation framework for the evaluation of industrial wireless networks in process control systems that could accommodate the diverse application domains and the unique QoS requirements encountered in this field.

This paper is among the first attempts to design industrial wireless networks in a CPS setting. We propose a simulation

Y. Liu and N. Moayeri are with Advanced Network Technologies Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, USA 20899 (e-mail: {yongkang.liu, nader.moayeri}@nist.gov).

R. Candell and K. Lee are with Intelligent Systems Division, Engineering Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, USA 20899 (e-mail: {richard.candell, kang.lee}@nist.gov).

U.S. Government work not protected by U.S. copyright

Liu, Yongkang; Candell, Richard; Moayeri, Nader; Lee, Kang.
"A Simulation Framework for Industrial Wireless Networks and Process Control Systems."
Paper presented at the 12th IEEE World conference on Factory Communication Systems - IEEE Transactions on Industrial Informatics, Aveiro, Portugal, May 3-May 6, 2016.

framework that integrates the process control system model and the wireless network model into a unified discrete-event simulator to study the interactions between the two components and evaluate the performance under joint system design. Specifically, we select a typical chemical production plant, i.e., the Tennessee Eastman Challenge (TE) Model, as the process system model. A widely used distributed controller proposed by Ricker is employed to operate the TE plant [14]. The control process requires the transmission of a variety of process variables (PVs) between the controller and the sensors/actuators on an ongoing basis. Accordingly, a protocol stack of an industrial wireless network based on the widely used WirelessHART standard is developed to model the wireless connections in the TE plant. The interactions between the process control system, i.e., the TE process and the controller, and the industrial wireless network are coordinated by the scheduling of periodic packet transmissions that carry the PV update information. Developed in the OMNET++ simulation platform [15], the simulation framework also supports extension with the external function modules developed in other OMNET++ simulation packages. We perform a case study using the TE model to evaluate the effects of imperfect wireless transmissions on the control system performance and develop link budgets and network-assisted control. The findings of this research help engineers to identify and mitigate the weaknesses of a wirelessly networked process control system.

The remainder of the paper is organized as follows. The related work is presented in Section II. The system model is introduced in Section III. A design for the simulation framework is proposed in Section IV. A performance evaluation based on the proposed framework along with issues related to wireless network design and implementation in process control systems are presented in Section V. Concluding remarks are given in Section VI.

II. Related Work

Wireless links in the harsh process control environment suffer from severe signal propagation loss and radio frequency (RF) interference. Remley et al. measured the wireless environment in a manufacturing plant and reported the significant differences compared to the indoor office environment [16]. Also based on field measurements, other research teams report vastly different radio wave propagation characteristics in different industrial applications depending on operating frequency [17] and factory topography [18]. Based on these findings, wireless solutions providing highly reliable and deterministic transmissions in wireless links for industrial control applications are proposed. To combat the uncertainty in wireless transmissions, reliable routing is proposed that introduces redundancy by using multiple paths for each traffic flow [19]. Since most industrial wireless networks coexist in the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) frequency band with other wireless technologies, such as Wi-Fi, co-channel interference is another major concern in network deployment [20]. Various interference mitigation techniques proposed include employing advanced scheduling schemes to reduce the intra-system interference [21] and probing multiple channels for transmission opportunities [22]. Industrial wireless network standards, such as WirelessHART [6], [23] and ISA100.11a [7], incorporate a variety of wireless technologies at different layers of their protocol stacks to guarantee deterministic control data delivery. These technologies include multi-channel hopping, blacklisting, and mesh networking with multi-path routing. It is of great interest to decide which one to select in deploying an industrial wireless network that would also take into account constraints such as transmission power, power consumption in case of battery-operated field instruments, plant layout, and other application-specific requirements. Our design of a simulation framework to analyze the behavior and performance of an industrial wireless network in conjunction with the underlying process control problem addresses many of these issues.

Computer-based simulations have been widely used in network design and analysis, which requires repeatable comparisons among various network scenarios and alternative solutions [24]. Simulations are also widely used to evaluate complex systems, such as cyber-physical systems, by co-simulating behaviors of component systems/networks in a hierarchical High-Level Architecture (HLA) [25], [26]. Event-driven simulators, such as NS2/NS3, OPNET and OMNET++, are developed for such purposes [28], [27]. As an open source software, the OMNET++ simulator provides a flexible language to depict various network behaviors and an extensible, modular, component-based framework to support different simulation projects [15]. Based on this powerful simulation engine, two frameworks named INET and MiXiM are proposed. While INET focuses on the modular simulation of the Internet protocol functions [29], MiXiM provides wireless and mobile simulation modules [30]. However, there are no existing simulation frameworks or functional modules for industrial wireless networks in OMNET++, just as there is no framework supporting simulation of process control systems and wireless networks together. In this paper, we develop an industrial network protocol stack with the OMNET++ engine and link it with the external functional modules, including the address resolution protocol (ARP) module in the INET library and the stochastic wireless channel model template in the MiXiM library, to provide comprehensive network simulations.

A well-designed process control application model can help the wireless engineer to better understand the needs of industrial wireless communications and validate the network design before deployment. Downs and Vogel developed the TE process model as a virtual chemical plant that has many attractive features in process control study, such as centralized control, networked sensors and actuators, multi-variable optimization, and performance metrics (mainly from the economic perspective) for scenarios with programmable setpoints [31]. It has been widely used in the verification of various plant control mechanisms and plant security discussions [32]. Ricker proposed several controllers for the TE model with objectives such as product rate control, quality control, and safety control [14], [33]. In these controller designs, the network connecting the controller with remote field instruments was assumed to be error-free and without

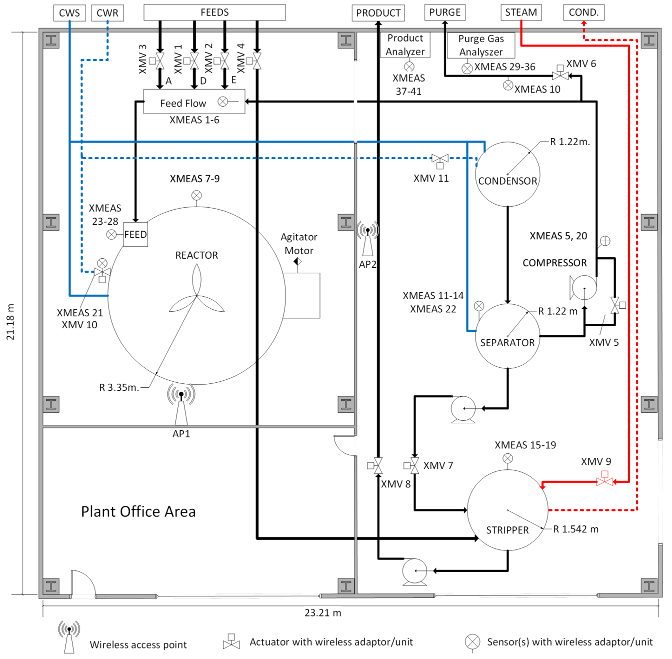


Fig. 1: A possible floor plan for the Tennessee Eastman Plant

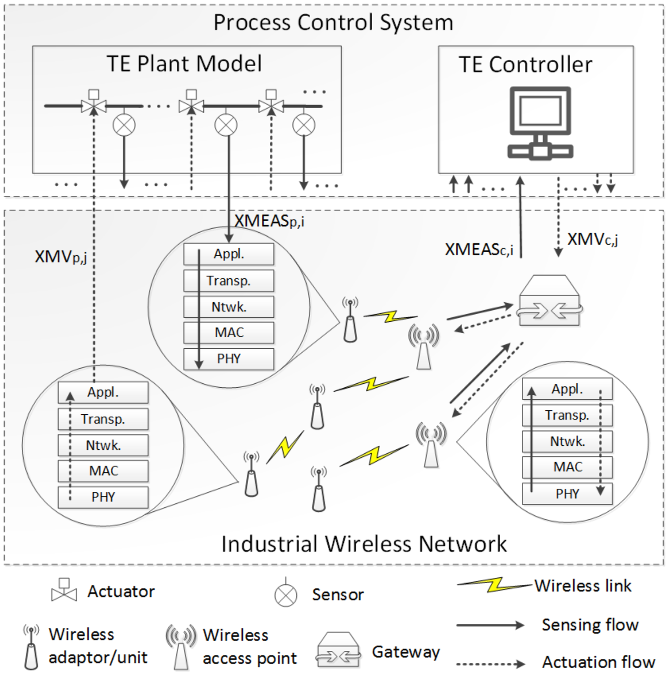


Fig. 2: Data flows in the simulation framework

any delay. When a wireless network is introduced in the plant operation, it becomes necessary to characterize the control data transmissions in the wireless links. In this paper, we adopt the TE model and Ricker's controller implemented in a wireless network setting and use the simulation approach to evaluate the effects of the wireless network on controller performance.

III. System Model

A. Factory Process Control Model

We choose the TE Model as the factory process control model in this paper [31]. Specifically, in the TE plant model, two liquid chemical products, denoted by G and H, are produced from four gaseous reactant inputs, denoted by A, C, D and E. There are one inert B and one byproduct F in the production process, both of which are also gaseous. As shown in Fig. 1, there are five operational units in the process, namely a reactor, a condenser, a vapor-liquid separator, a product stripper, and a recycle compressor. There are a total of 53 PVs available in the process, 41 of which are sensor measurements and 12 of which are manipulated variables, denoted by XMEASs and XMVs, respectively. The XMEASs indicate the instantaneous state of the process, such as temperatures, pressures, liquid levels, and chemical composition metrics. The PVs represent the control commands to various actuators, such as valve settings and coolant rates. The controller requires updates of the PV values in the plant operation on an ongoing basis to meet the production and safety requirements.

The selection of optimal controller for the TE plant is out of the scope of this paper. We choose one typical distributed controller model proposed by Ricker that uses the Euclidean solver for the TE plant control with non-linear differential equations. Interested readers are referred to [31] for the details of the reactions in this chemical process model and [14] for the controller design used in this paper.

B. Network Model in the TE Plant

As shown in Fig. 2, our industrial wireless network model consists of a gateway and several wireless access points and wireless nodes (i.e., sensors and actuators equipped with wireless adaptors). Beyond the gateway, the process control network and other network entities, e.g., security, office and asset management servers, that form the entire factory network are beyond the scope of this paper.

The gateway runs as the network manager that sets up the wireless links between the controller and the individual field instruments. The controller of the TE plant is running at the gateway and it is directly connected with all wireless access points (APs) through wired connections. The wireless nodes are distributed over the plant, either attached to the surfaces of the measured/manipulated objects or mounted on the pipes connected to them. Each wireless node is equipped with a half-duplex radio and associated with one or multiple PVs. For example, as shown in Fig. 1, the stripper-related XMEASs (XMEAS 15-19) share one wireless node at the same spot. However, each PV is allocated its own wireless bandwidth in a periodic manner to guarantee deterministic transmission within the network.

The controller requires periodic communications with the field instruments for the exchange of XMEAS and XMV PVs. To better identify different PV flows, each one carrying the XMEAS value from a sensor to the controller is denoted as a sensing flow and each one carrying the XMV value to an actuator is denoted as an actuation flow. The transmissions of PV flows in the wireless links are centrally coordinated by the gateway in such a manner that there is no interference between the wireless links in the industrial wireless network. However, alien systems may still interfere with the links of the industrial wireless network. The long-term ambient interference is incorporated in the noise level of the wireless channel model for the industrial environment. Other intermittent interference from nearby wireless nodes can be traced and mitigated through the co-existence solutions provided for example in [21], [22]. Additional information on wireless channel characterizations in the industrial plant environments can be found in [17], [18], [34].

IV. Design of the Simulation Framework

A. Overview

We choose the OMNET++ simulation library (written in C++) to build the simulation framework as a unified discrete-event simulator. The simulation framework incorporates the process control system and the industrial wireless network in the same OMNET++ project. As shown in Fig. 2, the framework is functionally divided into a process system simulator and a network simulator. As a global function module, the process system component can be further divided into two detached modules, the TE plant and controller, respectively. The former simulates the temporal evolution of the TE process. The latter computes the control decision based on the collected XMEAS PVs. These two modules don't connect directly to exchange PV values but through their respective interfaces to the wireless network simulator. In the wireless network simulator, the wireless node (the gateway) regularly checks the memory that stores the latest XMEAS (XMV) values from the TE plant (the controller) and updates the corresponding XMEAS (XMV) values at a separate memory at the controller (the TE plant). Each time an XMEAS (XMV) is updated and its new value is transmitted via the wireless network to the controller (the TE plant), the value of the corresponding PV at the destination is updated, if the network simulator indicates that the transmission was successful. Otherwise, i.e., if the transmission does not go through due to packet loss in the wireless link, long delay caused by retransmission or rerouting along different paths, the value of the PV is not updated and remains the same at the destination. The simulation framework makes it possible to (i) evaluate the effectiveness of the controller when imperfect wireless links are used for communicating PV values, and (ii) determine which wireless technologies, if any, can support control schemes used in delay-sensitive process control applications.

There are always some challenges in integrating a continuous-time process simulation, such as TESim, with a discrete-event network simulator, particularly when the time constants for one is in the order of hours and for the other in the order of milliseconds. We integrated the two simulations at the application layer. There are three options for the integration, namely, use of socket communications, direct call of an external C++ library, and use of embedded function modules. We opted for the third option. To maximize the overall simulation efficiency and speed, given the differences in time granularity between the two component simulations, we converted the TE Model into a global C++ function module and used the application layer of each communication node (sensor, actuator, or controller) as the interface to TE Model. Another challenge was that there were no models for the time division multiple access (TDMA) medium access control (MAC) protocol used in WirelessHART or PHY layer model based on appropriate channel propagation models in the OMNET++ library. To mitigate these issues, we implemented the WirelessHART MAC protocol and we used an appropriate IEEE reference channel model in OMNET++, as described in Sections IV-D and IV-E, respectively.

We had to make some tradeoffs in developing our simulation framework. Given that our focus was on studying the effects of wireless communications on the process control system, we had to make compromises on how we modeled timing and synchronization issues. For example, any transmitted process variable is assumed to be the instantaneous value acquired from the plant. Therefore, we did not consider sampling delay or quantization error in the acquisition process. In addition, the nodes in the wireless network are assumed to be synchronized all the time, which does not model collisions or missed messages due to asynchronous wake-up of field nodes. Furthermore, one can get more realistic simulation results by using a ray tracing engine to compute the RF channel impulse response between any pair of communicating nodes at any given time. However, that would have slowed down the simulations by orders of magnitude. As a compromise, we used the IEEE channel model mentioned above, but we took into account the distance between the two nodes and whether there was a line-of-sight (LOS) or non-line-of-sight (NLOS) propagation path between them.

In the following subsections, we discuss the details of the design of the simulation framework.

B. Coordination between Process and Network Simulations

The simulation of process events, which are mainly the fixed step updates of the PV values for the plant and the controller, is independent of the network simulation. The coordination between the two components is through management of the PV memories shared between the plant (controller) and the wireless node (gateway). For example, consider $\mathrm{XMEAS}_{\mathrm{p,i}}$, the sensing flow of the i-th XMEAS in the TE plant shown in Fig. 2. At each sensing moment, the plant module updates the value of $\mathrm{XMEAS}_{\mathrm{p,i}}$ and stores it in the memory shared with the network. In the timeslot allocated for the transmission of $\mathrm{XMEAS}_{\mathrm{p,i}}$, the wireless node fetches the updated value of $\mathrm{XMEAS}_{\mathrm{p,i}}$ from the shared memory, incorporates it as the payload into an application layer message, and passes it down to the physical radio module that in turn passes it to the gateway wirelessly. Upon reception at the application layer, the gateway updates the value of $\mathrm{XMEAS}_{\mathrm{c,i}}$ in the memory shared with the controller. Similar operations take place for the actuation flow from $\mathrm{XMV}_{\mathrm{c,j}}$ at the gateway to $\mathrm{XMV}_{\mathrm{p,j}}$ at the actuator.

The simulation modules are all synchronized to the simulation clock driven by the central event queue in the simulator core. The simulator core processes one event with the current timestamp from the event queue at a time and inserts new events with present or future timestamps into the queue. The fixed step process and control updates are managed by two separate timers, each of which is reloaded to the next update moment after the latest update, as shown in Fig. 3.

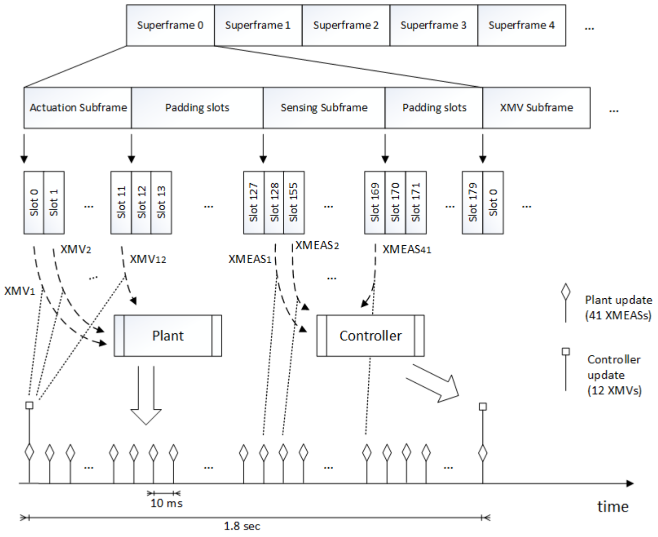


Fig. 3: Coordinations between slotted packet transmissions and PV updates

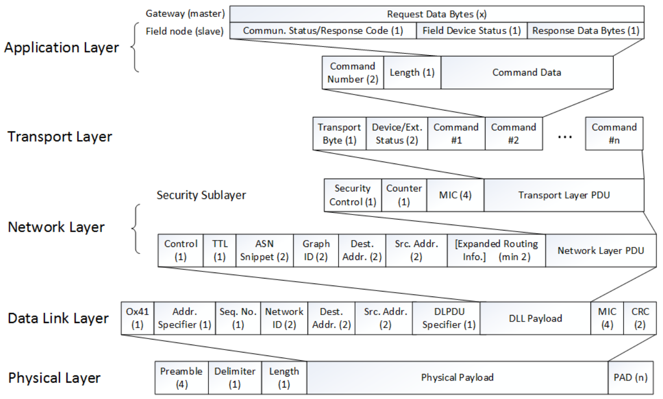


Fig. 4: WirelessHART protocol stack and inter-layer message frame structures with overhead counts

As suggested by Ricker, each PV gets one update every 1.8 second [14]. On the other hand, the network events are sorted by the timeslots and superframes along the timeline. The timeslot is the basic scheduling unit of length of 10 ms in the WirelessHART specification. One packet can be transmitted in one timeslot over a wireless link. The superframe, which is of the same length as the controller update period, i.e., 1.8 second, consists of multiple adjacent timeslots and it gets repeated periodically over time. The TDMA framing and scheduling in the WirelessHART network simulation will be discussed in more depth in Subsection IV-D.

C. *WirelessHART Network Simulation*

The wireless network simulator is based on the WirelessHART standard. As shown in Fig. 4, the WirelessHART protocol stack resembles the standard open systems interconnection (OSI) 7-layer protocol stack, but it consists of five layers, namely the application layer, the transport layer, the network layer, the data link layer (DLL), and the physical (PHY) layer. The detailed functional descriptions of these layers can be found in [6] and [35].

To facilitate performance evaluations, the network simulator enables key functions in individual layer modules and leaves open interfaces for future extensions. Specifically, the application layer module mainly serves as the interface with the TE process and controller modules. Command 33 (Read Variable Command) and Command 79 (Write Variable Command) of the HART communication commands are used in the simulations as the application layer messages in the update of PVs [4]. At the transport layer, multiple commands can be concatenated into one payload to reduce the control overhead and conserve bandwidth. At the network layer, the source node maintains the primary and alternative backup paths to the destination node in the routing table identified by the PV number. The mapping between the network ID and the node's MAC ID in the DLL is performed by the third party ARP module from the INET simulation package as a global function module [29]. The TDMA MAC design in the DLL module is presented in Subsection IV-D. The physical radio module is designed based on the template provided in the MiXiM wireless simulator package [30]. We have the capability to introduce new wireless channel models based on field measurement in a real plant environment. The modular design of the network simulator masks the details of the layer functions in individual protocols and encourages interchangeable reuse of the layer modules, which facilitates comparisons of various network designs using any of a number of choices at each protocol stack layer.

The information exchange between adjacent layers in the protocol stack is through messages with packet formats shown in Fig. 4. At the transmitter, e.g., the AP for the actuation flow in Fig. 2, each layer module treats the upper layer message as the payload and encapsulates it with its own control information as header to form the message packet and sends it down to the next lower layer. At the receiver, e.g., the actuator with the same flow in Fig. 2, in a bottom-up manner, each layer module acquires the information from the packet header sent by its peer layer in the AP and forwards the payload to the upper layer. Between the peer layers of two wireless nodes, the control information in the packet header, such as the routing information in the network layer and the MAC address in the DLL as shown in Fig. 4, are interpreted and used for the specific layer functions.

D. *TDMA MAC Layer Design*

The main function of the WirelessHART DLL is the MAC protocol which allocates the radio resources to the transmissions in wireless links. The radio resources spread over time and frequency domains.

In the time domain, WirelessHART adopts the time division multiple access (TDMA) scheme to provide timely transmissions. Other industrial wireless networks, such as ISA100.11a, use the same approach. A timeslot, of duration 10 ms, is the smallest allocation of time in the TDMA MAC that supports one handshake in a wireless link including the transmission of one MAC packet and its ACK/NACK reply. As explained in Subsection IV-B, each PV update will get its own exclusive timeslot for each of the links along the end-to-end path. Each

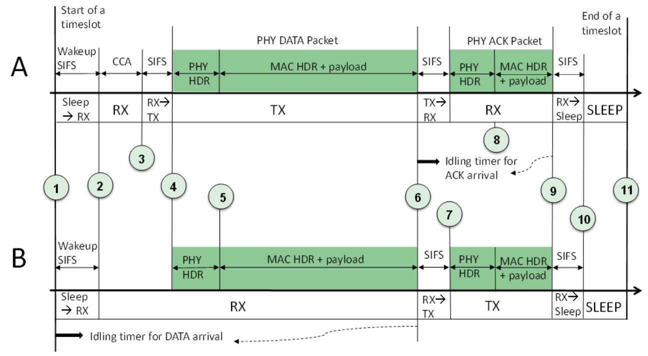


Fig. 5: Transmitter and receiver simulation events in a WirelessHART timeslot

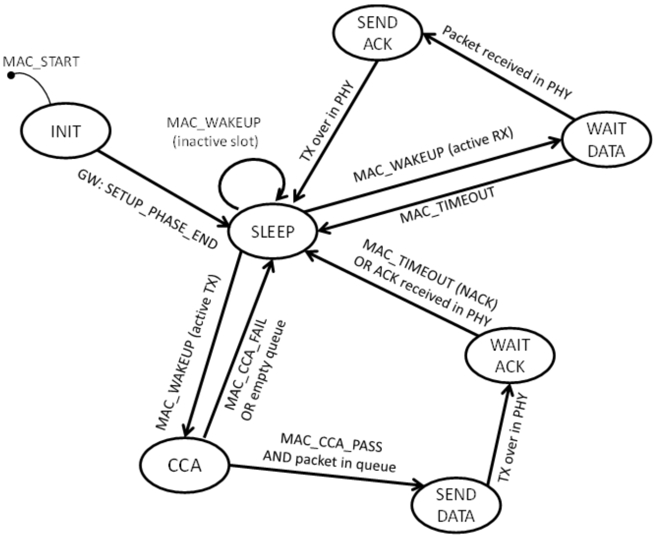


Fig. 6: Finite State Machine (FSM) representation of the WirelessHART TDMA MAC

transmission over the link is mapped to a unique timeslot with the same offset to the beginning of each superframe, which is maintained by a global schedule at the network manager. At the beginning of a timeslot, every wireless node checks the schedule. During each timeslot only the radios at the transmitting and receiving nodes are activated and they follow the procedures shown in Fig. 5. The MAC layer carries out certain tasks according to radio state and PHY layer framing and it responds to various events at different time instances. For example, consider transmission of a packet from node A to node B. At the time instance labeled 2 in Fig. 5, the transceivers at both A and B switch to the receiving state. The transceiver at A is performing carrier sensing in the clear channel assessment (CCA) state. The transceiver at B switches to the WAIT DATA state to receive the signal carrying the data packet. At the time instance labeled 6, i.e., at the completion of the data packet transmission, the transceiver at A switches to the receiving state to wait for the ACK packet and it enables the idling timer. Meanwhile, the transceiver at B stops its idling timer for the data packet and switches to transmit state to send the ACK/NACK packet. The transceiver at A will go to sleep to save energy if the idling timer expires before it is disabled by any expected packet arrival and the scheduled event of sending an ACK by B will be removed from the schedule. To depict various events and actions associated with the transceiver states and the roles various nodes play, a finite state machine for the WirelessHART MAC module is developed and shown in Fig. 6.

In the frequency domain, WirelessHART nodes work in the 2.4 GHz ISM band using the IEEE 802.15.4 radio. The WirelessHART network can employ up to 15 non-overlapping wireless channels, each with a 2 MHz bandwidth and separated from adjacent channels by a 5 MHz spacing. WirelessHART not only allocates timeslots to a given link in a periodic manner using the superframe structure, but it also uses channel hopping by assigning various channels to the same link to provide channel diversity. Specifically, the channel assigned to link l at timeslot t is given by

$$c_l(t) = T_{hop}((ASN_t + c_l) \text{ mod } |C_a|) \tag{1}$$

where $|C_a|$ is the size of the active channel set, c_l is the original channel offset for link l, and ASN_t is the absolute slot number (ASN) of the current timeslot t since ASN 0 when the network was created. $T_{hop}(i)$ is the lookup table for channel hopping sequence with a static pseudo-random mapping between the inputs from 0 to $|C|$ [36]. Note that the set of active channels may be a proper subset of all 15 possible channels, due to the blacklisting rules that prohibit the use of some severely interfered channels.

E. Empirical Industrial Wireless Channel Model

To simulate the transmissions in the industrial environment, we employ an empirical industrial wireless channel model in the physical layer. Generally, the channel model consists of a large scale path loss model, a shadow fading component, and a small scale fading component. Specifically, as a function of the distance d between the transmitter and the receiver, the signal power P_r at the receiver can be written in the logarithmic form as

$$P_r = P_t + PL(d) \tag{2}$$

where P_t is the transmit power level, and PL is the path loss model, which can be modeled as

$$PL = PL_0 + 10n\ log_{10}(d/d_0) + X \tag{3}$$

where PL_0 is the path loss at the reference distance d_0, n is the path loss exponent, and the shadow fading component X is a Gaussian random variable in decibel, $X \sim N(0, \sigma^2)$. As noted in [34], depending on whether the link is Line-of-Sight (LOS) or Non-Line-of-Sight (NLOS), different values are used for n, σ^2 and different lookup tables are used to obtain packet error rate (PER) as a function of signal-to-noise-ratio (SNR).

We use E_b/N_0 as the link quality metric given by

$$\frac{E_b}{N_0} = \frac{C}{N} \cdot \frac{B}{R} \tag{4}$$

where C is the carrier signal power after the receiver filter but before detection including the noise figure of the receiver, N is the noise power at the receiver, B is the bandwidth and R is the channel data rate.

TABLE I: LOS/NLOS PER Table (Packet size: 64 Bytes)

E_b/N_0	$P_{e,nlos}$	$P_{e,los}$	E_b/N_0	$P_{e,nlos}$	$P_{e,los}$
0 dB	1.0000	1.0000	22 dB	0.5102	0.0606
2 dB	1.0000	1.0000	24 dB	0.4348	0.0420
4 dB	1.0000	1.0000	26 dB	0.2488	0.0308
6 dB	1.0000	1.0000	28 dB	0.1786	0.0163
8 dB	1.0000	1.0000	30 dB	0.1196	0.0106
10 dB	1.0000	0.9615	32 dB	0.0627	0.0073
12 dB	1.0000	0.7246	34 dB	0.0452	0.0041
14 dB	1.0000	0.4545	36 dB	0.0284	0.0024
16 dB	0.9804	0.3623	38 dB	0.0174	0.0016
18 dB	0.8475	0.1923	40 dB	0.0106	0.0012
20 dB	0.6667	0.1121	42 dB	0.0096	0.0000

TABLE II: Simulation Parameters

Number of XMEASs	41
Number of XMVs	12
Plant update period	1.8 s
Controller update period	1.8 s
Plant simulation time	72 hrs
Number of APs	2
timeslot	10 ms
Superframe size	180 timeslots
Number of channels	15
Per channel bandwidth	2 MHz
data rate	250 kbps
PHY Data packet size	64 Bytes
PHY ACK packet size	20 Bytes
Transmitter power	-10 dBm
Receiver noise figure	11 dB
Path loss model	IEEE industrial [34]
CCA length	192 μs
Radio wakeup time	684 μs
SIFS	192 μs

Each time a packet is transmitted, the physical layer module in the receiver calculates the value of E_b/N_0 using the link length, link type, and packet size, and then maps this value to the corresponding PER value and decides whether the packet has been received correctly or not by flipping a coin. Table I shows the PER table used in the simulator for both LOS and NLOS links.

V. Performance Evaluation

A. General Simulation Setting

We design three sets of experiments to evaluate the impact of the wireless channel on the process control system, the wireless network setup/configuration, and the coordination between wireless network and the process control system. In these experiments, the TE controller manages the plant to operate at the optimal setpoints in Mode 1, where the production rates for products G and H are the same [31]. Table II enumerates the parameters for the simulation and the typical values used in these experiments. The TE plant library and the simulation framework are maintained in the GitHub repositories [37] and [38].

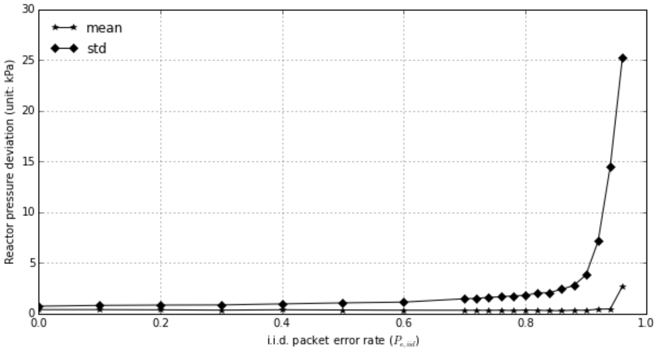


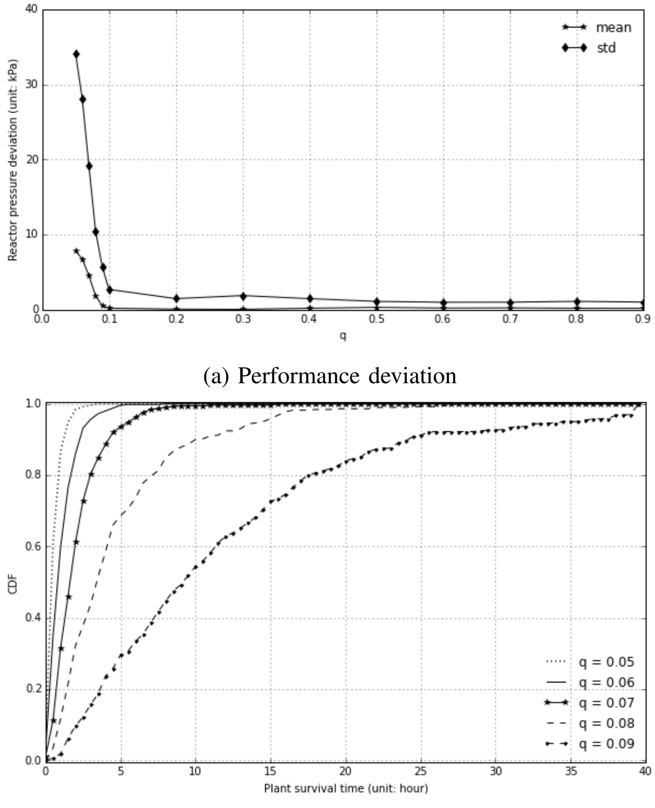
Fig. 7: Performance deviation under different packet error rates in IID channel model

B. Effects of Packet Errors on the TE Plant

We start by studying the impact of wireless packet transmission errors on the process control performance before considering the networking issues. We assume that each field instrument is connected to the controller through a direct wireless link. Two stochastic channel models are used to model random link failures, i.e., the independent and identically distributed (IID) packet loss model and the two-state Gilbert-Elliot (GE) channel model [39], [40]. Among the many operational objectives for the TE plant, we select the reactor pressure as the performance metric because it is particularly vulnerable to imperfect control command communications. Although a higher reactor pressure is preferred because it accelerates the reactions for the products, the TE process will shut down the plant for safety reasons if the reactor pressure exceeds 3000 kPa. The setpoint for the reactor pressure is set at 2800 kPa as suggested by [14].

With the IID channel model, the wireless PV updates are statistically independent of each other and the packet error rate is the same at all times. As each PV gets updated in a superframe, a larger PER $P_{e,iid}$ makes it more likely for the packets to get impaired and dropped, which causes the controller to take more time to acquire the process status and respond to any disturbances. Fig. 7 shows the mean and standard deviation of reactor pressure from its setpoint as a function of $P_{e,iid}$. Each point in Fig. 7 represents 100 repeated experiments with random seeds. The results indicate that the reactor pressure control deviates more from the setpoint as the communication channel gets less reliable, which may result in a plant shutdown.

Next we look at the GE channel model, which is designed to model bursty losses in wireless links with two recurring states [39], [40]. In this paper, we assume that each wireless link in the experiment follows the GE model and jumps between the good state and the bad state with the transition probabilities p and q, respectively. We assume that in the good state a packet gets transmitted over the channel without any errors with 100% probability and in the bad state it gets blocked with 100% probability. Therefore, the average PER in



(a) Performance deviation

(b) CDF of plant survival time

Fig. 8: Performance of TE plant under different bursty packet losses in GE channel model ($P_{e,GE} = 0.6$)

the GE model is $P_{e,GE} = p/(p+q)$ and the average sojourn time in the good (bad) state is T/p (T/q), where T is the PV update period, i.e., 1.8 second in the Ricker's controller. A smaller q means a longer interval between successive updates over a wireless link, which reduces the agility of the controller and postpones the manipulation effort. Fig. 8a illustrates the mean and standard deviation of pressure deviation as a function of q while the average PER is kept at 0.6. Meanwhile, as there is a significant deviation of the reactor pressure when $q < 0.1$, the plant shuts down rapidly within a few hours. The smaller q is, the faster the shutdown happens. Fig. 8b verifies this with the cumulative distribution function (CDF) of the plant survival time, i.e., the time until shutdown, for different q at the same average PER of 0.6.

C. Industrial Wireless Network Setup and Configuration

In the second experiment, we evaluate the simulation framework as a supporting tool for network setup and configuration. The installation and maintenance of the wireless network in an industrial plant is usually managed by the plant information technology (IT) engineers. In case of a WirelessHART network, each wireless node is manually configured through the WirelessHART handheld field communicator [6]. Therefore, a study of the procedures in the installation and maintenance of industrial wireless networks is of special interest.

AP Site Selection

The radios of field instruments are normally installed next to the sensing/actuation parts that are typically placed at fixed locations. As the wireless links are established between the field nodes and the APs, the APs can better serve the areas they cover if their sites are carefully selected during network deployment. In this experiment, we probe for the possibility of link improvement in the simulation platform. As shown in Fig. 1, the total TE plant area can be divided into three major sectors, namely, the reaction sector (the upper left half), the product separation sector (the right half), and the office area (the lower left half). Two APs, AP1 and AP2, are deployed to serve the reaction sector and the separation sector, respectively. Each AP is associated with the wireless field instruments placed in its serving sector. Considering the availability of wired network docks and power grid supply, AP1 is mounted on the wall between the reaction sector and the office area with coordinate range ([2.5 m:11.60 m], 7 m, [1.6 m:6.5 m]) in Fig. 1, and AP2 is mounted on the wall between the reaction sector and the separation sector with coordinate range (11.75 m, [7 m:16.5 m], [1.6 m:6.5 m]). Therefore, the locations of the antennas on the mounting walls are programmable in the AP site selection procedure.

We measure the impact of the AP site on the wireless links it serves by finding the worst PER link in the coverage area as given by

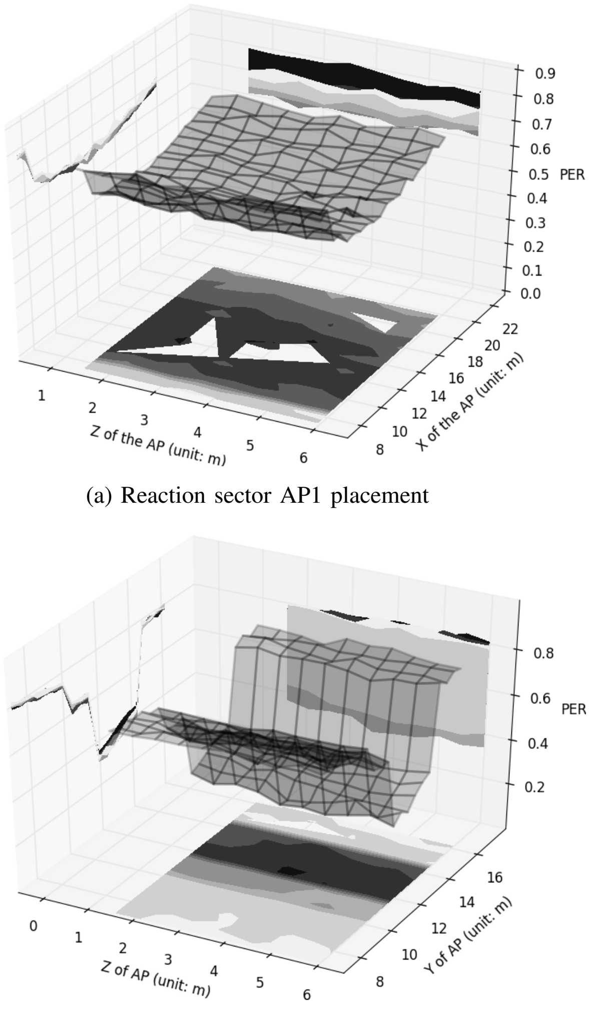
$$P_{e,j} = \max_{l \in L_j} P_{e,l} \quad for\ j \in \Theta, \tag{5}$$

where Θ is the set of all possible AP positions, L_j is the set of links between the AP at a site j and its wireless nodes, and $P_{e,l}$ is the PER for link l.

To optimize the AP placement, the objective can be written as

$$\underset{j \in \Theta}{\operatorname{argmin}}\ P_{e,j} \tag{6}$$

At each candidate position, the AP broadcasts 1000 messages at the regular transmission power and each wireless node counts the number of successful receptions, from which $P_{e,l}$ for various links are computed and reported to the network manager, which collects the $P_{e,j}$ measured at each site and decides the best AP sites in both sectors. Fig. 9 illustrates the distribution of $P_{e,j}$ for AP1and AP2 in the reaction sector and the separation sector, respectively. It is observed that the floor plan of the plant has a significant effect on the wireless links and the network performance. In the reaction sector, there is a huge reactor tank that introduces significant shadow fading in some links and causes higher PER in the links no matter where AP1 is placed on the mounting wall. The separation sector, on the other hand, houses smaller sized equipment. Hence, if AP2 is placed at certain locations, it can connect with every field instrument with a good link. As shown in Fig. 9b, when AP2 is positioned at (11.75 m, 11.5125 m, 4.54 m), it can achieve the minimum $P_{e,j}$ of 0.225. As mentioned in previous experiments, if the link PER is 0.225 or lower, the TE controller can easily manage the process and meet the objectives.



(a) Reaction sector AP1 placement

(b) Product separation sector AP2 placement

Fig. 9: Distribution of $P_{e,j}$ in the TE plant with AP placement

Link Improvements

Once the APs have been installed, "softer" mechanisms can be used in the wireless network to further enhance the links. In many cases, the link between an AP and a field instrument is NLOS, which results in higher PER and potentially requiring a number of retransmissions. Multi-hop transmissions can be enabled at the network layer by the routing function to detour the heavily faded areas. In addition, link redundancy can be introduced at the DLL by allocating retransmissions for any PV update. Specifically, a routing metric, e.g., the expected transmission count (ETX), is used to determine the best path between the wireless node and the associated AP in the sense of minimizing ETX [41]. The PV update is then transmitted to the AP along that best path. For example, in the reaction sector in Fig. 1, the feed flows, XMEAS 1-6, have poor NLOS links with AP1, and the average PER for direct connections is 0.759. Accordingly, the ETX value is $1/(1 - Pe) = 4.419$, implying that on the average the direct link requires 4.419 transmissions over that many timeslots to transmit one PV update successfully. When the ETX routing is applied, the feed flows can reach AP1 via the relay at the wireless node that can carry the transmissions of XMEAS 23-28 and XMV 10. The ETX in the 2-hop path turns out to be 2.642. The resources allocated for each PV flow for the (re-)transmission along the path are scheduled in adjacent timeslots in each superframe using a scheduling scheme such as [42]. Fig. 10 illustrates the improvements in the PV update process by introducing retransmissions and multi-hop routing in the industrial wireless network. Therefore, full mesh-like topology in the WirelessHART network and retransmissions in the wireless links can improve the PV update performance in the TE process. When retransmissions are not used, the method of sending PV updates over direct links require 53 timeslots in each superframe and the method using multi-hop transmissions requires 63 timeslots to allow some 2-hop relay links in each transmission round. Naturally, retransmissions increase the total amount of resources required to update the PVs.

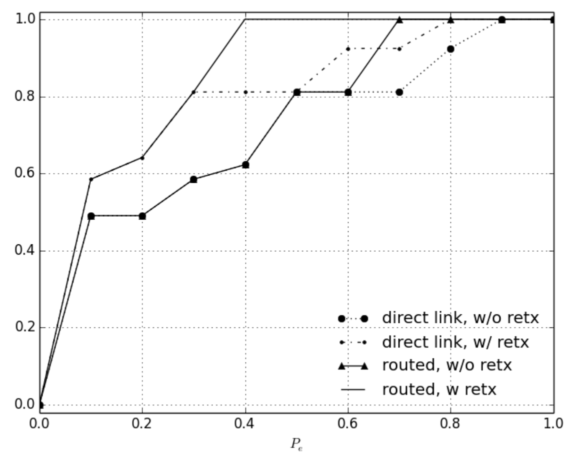
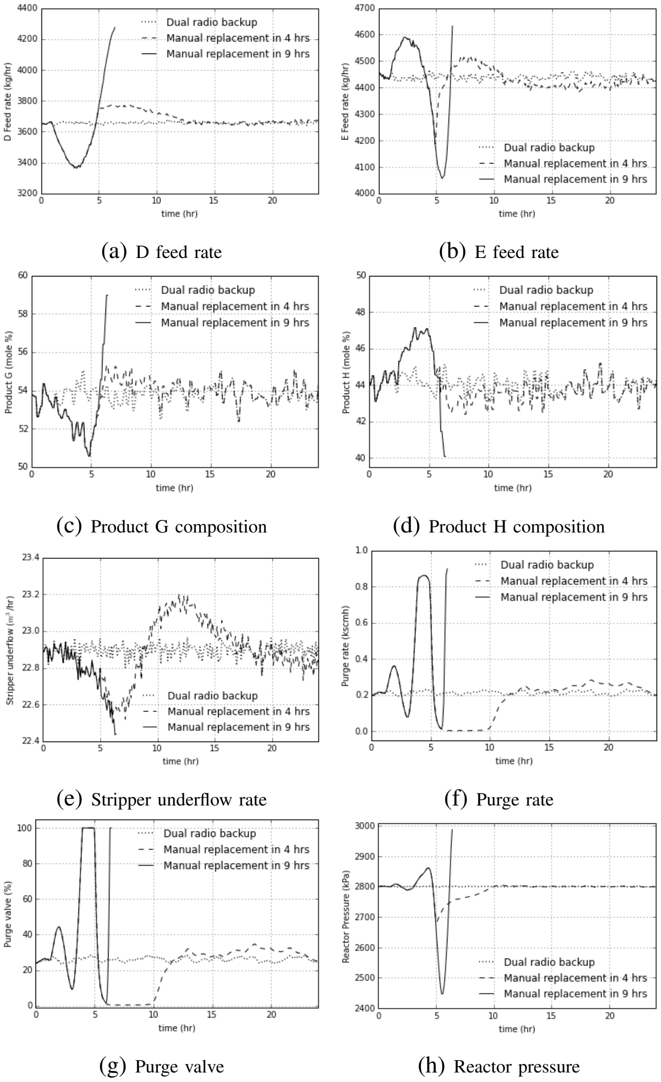


Fig. 10: Fraction PVs (out of a total of 53) for which probability of end-to-end transmission failure is smaller than or equal to P_e

D. *Effects of Network Operation on the TE Plant Performance*

The developed simulation enables the interdisciplinary study of the physical process and the network. In the final experiment, we evaluate the impact of the response time to wireless network failures on the control performance. We simulate the case where a wireless link is lost due to battery problems or radio failure, which delays PV updates and in turn results in the deviation of the process from the control setpoints. Fig. 11 illustrates the simulation results in one possible case that the primary radio of the wireless node in charge of updating the feed rates, i.e., XMEAS 1-6, goes down one hour into the simulation. Several options are available to detect and fix this link problem. In the WirelessHART standard, the network manager can routinely check the field devices through Command 41 (Perform Self Test) messages. If the node does not respond to this message, the communication link may be lost. In the TE plant, such polling can be performed every minute or less frequently. The network manager can count



(a) D feed rate

(b) E feed rate

(c) Product G composition

(d) Product H composition

(e) Stripper underflow rate

(f) Purge rate

(g) Purge valve

(h) Reactor pressure

Fig. 11: PV variations in the simulations of link failure and recovery for the feed flow rate updates (XMEAS 1-6)

the non-responses over a sliding time window, e.g., 5 min, to identify the failure in the wireless link and take action to mitigate the problem by invoking the backup radio, for example.

As shown in Fig. 11, when dual radios are installed in each wireless node, the network-based link monitoring scheme can invoke the backup radio and bring the PV update back to the schedule in a few minutes. The performance degradation with respect to regular operation is minor. Compared with this embedded network solution, the alternative control-based solution needs to continuously monitor the process and send alerts upon detection of abnormal PV variations. However, as many inherent process disturbances or control system failures may also cause similar variations in the process, it usually takes longer for the plant staff to locate the problem and fix it. In the TE plant, extended absence of updated feed rates causes the TE plant to suffer from significant variation in the production, as shown in Fig. 11e, changes in product compositions, as shown in Fig. 11c and Fig. 11d, or increasing the risk that the controller shuts down the process due to high reactor pressures, as shown in Fig. 11h.

VI. Conclusions

In this paper, we have proposed a novel simulation-based evaluation framework for industrial wireless networks intended for use in process control systems. Focusing on the control-centric data flows, the framework coordinates the simulations on both sides and serves as a powerful tool in the study of the process control systems, network configuration, and the joint system design. In future work, we will study generic interface design in the framework to integrate other physical systems, such as robot control, with the wireless network for performance and safety improvements.

Disclaimer

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

References

[1] R. R. Rajkumar et al. “Cyber-physical systems: the next computing revolution,” in *Proceedings of the ACM 47th Design Automation Conference*, 2010.

[2] J. H. Lee and J. M. Lee, “Progress and Challenges in Control of Chemical Processes,” *Annu. Rev. Chem. Biomol. Eng.*, Vol. 5, No. 1, pp. 383-404, 2014.

[3] H-J K¨rber, H. Wattar and G. Scholl, “Modular wireless real-time sensor/actuator network for factory automation applications”, *IEEE Transactions Industrial Informatics*, Vol. 3, No. 2, pp. 111–119, May 2007.

[4] HART Communication Foundation, “Common Practice Command Specification,” HCF_SPEC-151, Rev. 8.0, Apr. 2001.

[5] J. Song et al. “WirelessHART: Applying wireless technology in real-time industrial process control”, in *Proceedings of the IEEE RTAS’08*, 2008.

[6] IEC 62591 Ed. 1.0 b:2010, “Industrial Communication Networks - Wireless Communication Network and Communication Profiles - WirelessHART^{TM},” 2010.

[7] “Wireless Systems for Industrial Automation: Process Control and Related Applications”, ISA-100.11a-2009 Standard, 2009.

[8] A. K. Somappa, K. Øvsthus and L. M. Kristensen, “An Industrial Perspective on Wireless Sensor Networks: A Survey of Requirements, Protocols, and Challenges,” *IEEE Commun. Surv. Tutor.*, Vol. 16, No. 3, pp. 1391-1412, 2014.

[9] K. J. Åström et al. “Automatic tuning and adaptation for PID controllers-a survey,” *Control Engineering Practice*, Vol. 1, No. 4, pp. 699–714, 1993.

[10] I. F. Akyildiz et al. “Wireless sensor networks: a survey,” *Computer networks*, Vol. 38, No. 4, pp. 393–422, 2002.

[11] B. P. Zeigler, H. Praehofer and T. G. Kim, “Theory of modeling and simulation: integrating discrete event and continuous complex dynamic systems”, Academic press, 2000.

[12] T. Godfrey et al. “Modeling smart grid applications with co-simulation,” in *Proceedings of the IEEE SmartGridComm’10*, 2010.

[13] C. Sommer, R. German and F. Dressler,“Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis,” *IEEE Transactions on Mobile Computing*, Vol. 10, No. 1, pp. 3–15, January 2011.

[14] N. L. Ricker, “Decentralized Control of the Tennessee Eastman Challenge Process”, *J. Proc. Cont.*, Vol. 6, No. 4, pp. 205–221, 1996.

[15] “OMNET++ Discrete Event Simulator”,
Available at https://omnetpp.org/

[16] K. Remley et al. “NIST Tests of the Wireless Environment in Automobile Manufacturing Facilities”, *NIST Technical Note 1550*, 2008.

[17] E. Tanghe et al. “The Industrial Indoor Channel: Large-Scale and Temporal Fading at 900, 2400, and 5200 MHz”, *IEEE Transactions on Wireless Comm.*, Vol. 7, No. 7, pp. 2740–2751, Jul. 2008.

[18] J. Ferrer-Coll et al. “Characterisation of highly absorbent and highly reflective radio wave propagation environments in industrial applications,” *IET Communications*, Vol. 6, No. 15, pp. 2404–2412, 2012.

[19] S. Han et al. “Reliable and Real-Time Communication in Industrial Wireless Mesh Networks”, in *Proceedings of IEEE RTAS’11*, 2011.

[20] L. L. Bello and E. Toscano, “Coexistence issues of multiple co-located IEEE 802.15. 4/ZigBee networks running on adjacent radio channels in industrial environments”, *IEEE Transactions on Industrial Informatics*, Vol. 5, No. 2, pp. 157–167, 2009.

[21] S. Lv et al. “Understanding the scheduling performance in wireless networks with successive interference cancellation,” *IEEE Transactions on Mobile Computing*, Vol. 12, No. 8, pp. 1625–1639, Aug. 2013.

[22] H.T. Cheng and W. Zhuang, “Simple channel sensing order in cognitive radio networks,” *IEEE Journal on Selected Areas of Communications*, Vol. 29, No. 4, April 2011.

[23] S. Petersen and S. Carlsen, “Performance evaluation of WirelessHART for Factory Automation,” in *Proceerdings of IEEE ETFA’09*, pp. 1–9, 2009.

[24] B. Li, L. Nie, C. Wu, H. Gonzalez, and C. Lu, “Incorporating Emergency Alarms in Reliable Wireless Process Control,” in *Proc. ICCPS’15*, 2015.

[25] H. Neema, et. al. “Model-Based Integration Platform for FMI Co-Simulation and Heterogeneous Simulations of Cyber-Physical Systems,” in *Proc. 10th International Modelica Conference*, 2014.

[26] E. Galli, G. Cavarretta and S. Tucci, “HLA-OMNET++: an HLA compliant network simulation,” in *Proc. DS-RT’08*, pp. 319-321, 2008.

[27] F. Bause, P. Buchholz, J. Kriege and S. Vastag, “A Simulation Environment for Hierarchical Process Chains Based on OMNeT++,” *Simulation*, Vol. 86, No. 5-6, pp. 291-309, May/June 2010.

[28] P. Zand et al. “Implementation of WirelessHART in the NS-2 Simulator and Validation of Its Correctness”, *Sensors*, Vol. 14, No. 5, pp. 8633–8668, May 2014.

[29] “INET Framework”, Available at https://inet.omnetpp.org/

[30] A. Köpke et al. “Simulating Wireless and Mobile Networks in OMNET++ The MiXiM Vision,” in *Proceedings of Simutools’08*, 2008

[31] J. J. Downs and E. F. Vogel, “A Plant-wide Industrial Process Control Problem”, *Comput. Chem. Engng.*, Vol. 17, No. 3, pp. 245–255, 1993.

[32] Alvaro Cardenas et al., “Attacks Against Process Control Systems: Risk Assessment, Detection, and Response,” in *Proceedings of ASIACCS’11*, Hong Kong, China, 2011.

[33] N. Lawrence Ricker. “New Simulink models of two decentralized control strategies,” Available at http://depts.washington.edu/control/LARRY/TE/download.html#Multiloop

[34] A. F. Molisch et al. “IEEE 802.15.4a channel model-final report”, IEEE P802 15.04, Nov. 2004.

[35] D. Chen, M. Nixon and A. Mok, “WirelessHART^{TM} Real-Time Mesh Network for Industrial Automation”, Springer, 2010.

[36] K. S. J. Pister and L. Doherty, “TSMP: Time Synchronized Mesh Protocol,” in *Proc. DSN’08*, Orlando, FL, USA, Nov. 2008.

[37] NIST, “Tennessee Eastman simulation,” GitHub, Available at https://github.com/usnistgov/tesim, 2015.

[38] NIST, “Tennessee Simulator federated with OMNET++ networking model,” GitHub, Available at https://github.com/usnistgov/tesim_omnetpp, 2015.

[39] E. N. Gilbert, “Capacity of a Burst-Noise Channel”, *Bell Syst. Tech. J.*, Vol. 39, pp. 1253–1265, Sept. 1960.

[40] E. O. Elliott, “Estimates of Error Rates for Codes on Burst-Noise Channels”, *Bell Syst. Tech. J.*, Vol. 42, pp. 1977–11997, Sept. 1963.

[41] S. Biswas, R. Morris, “ExOR: Opportunistic Multi-hop Routing for Wireless Networks,” *ACMSIGCOMM Computer Communication Review*, Vol. 34, No. 1, pp. 133–144, 2005.

[42] A. Saifullah, Y. Xu, C. Lu and Y. Chen, “End-to-End Communication Delay Analysis in Industrial Wireless Networks”, *IEEE Transactions on Computers*, Vol. 64, No. 5, pp. 1361–1374, May 2015.

Effects of Wireless Packet Loss in Industrial Process Control Systems

Yongkang Liu, Richard Candell, and Nader Moayeri

National Institute of Standards and Technology, Gaithersburg MD, U.S.A
[yongkang.liu, richard.candell, nader.moayeri]@nist.gov

Abstract — Timely and reliable sensing and actuation control are essential in networked control. This depends on not only the precision/quality of the sensors and actuators used but also on how well the communications links between the field instruments and the controller have been designed. Wireless networking offers simple deployment, reconfigurability, scalability, and reduced operational expenditure, and is easier to upgrade than wired solutions. However, the adoption of wireless networking has been slow in industrial process control due to the stochastic and less than 100 % reliable nature of wireless communications and lack of a model to evaluate the effects of such communications imperfections on the overall control performance. In this paper, we study how control performance is affected by wireless link quality, which in turn is adversely affected by severe propagation loss in harsh industrial environments, co-channel interference, and unintended interference from other devices. We select the Tennessee Eastman Challenge Model (TE) for our study. A decentralized process control system, first proposed by N. Ricker, is adopted that employs 41 sensors and 12 actuators to manage the production process in the TE plant. We consider the scenario where wireless links are used to periodically transmit essential sensor measurement data, such as pressure, temperature and chemical composition to the controller as well as control commands to manipulate the actuators according to predetermined setpoints. We consider two models for packet loss in the wireless links, namely, an independent and identically distributed (IID) packet loss model and the two-state Gilbert-Elliot (GE) channel model. While the former is a random loss model, the latter can model bursty losses. With each channel model, the performance of the simulated decentralized controller using wireless links is compared with the one using wired links providing instant and 100 % reliable communications. The sensitivity of the controller to the burstiness of packet loss is also characterized in different process stages. The performance results indicate that wireless links with redundant bandwidth reservation can meet the requirements of the TE process model under normal operational conditions. When disturbances are introduced in the TE plant model, wireless packet loss during transitions between process stages need further protection in severely impaired links. Techniques such as retransmission scheduling, multipath routing and enhanced physical layer design are discussed and the latest industrial wireless protocols are compared.

Keywords — industrial control systems, chemical process control, process resilience, process performance, measurement science, testbed, safety

Liu, Yongkang; Candell, Richard; Moayeri, Nader.
“Effects of Wireless Packet Loss in Industrial Process Control Systems.”
Paper presented at the 2015 ISA Process Control & Safety Symposium, Houston, TX, Nov 9-Nov 12, 2015.

I. Introduction

Industrial process control is a control problem where various sensing and automation technologies are used to supervise the production activities in a plant. In the past few decades, the use of process control has been growing rapidly in conjunction with various plant management systems, such as inventory management, product quality check, plant safety monitoring and environmental control, for optimizing the entire plant operation [1]. In industrial process control, control strategies are generally built around organizing sensing and actuation to serve comprehensive and complicated control tasks. The control data in process control mainly consists of process variables (PVs) and manipulated variables (MVs), the former being the data acquired from field sensors and the latter the commands that need to be applied to actuation devices. In order to achieve the control objectives, the control data needs to be reliably communicated over secure communications links.

Wired communications has been traditionally adopted for use in control systems, because it provides direct, reliable connections between field instruments and control units by wires/cables, multiplexers and fieldbus protocols. However, wired communications has its own limitations. For example, wired connections do not scale well or support network reconfiguration as the process control evolves, larger networks need to be supported, or more data is generated. As an alternative solution, field instruments equipped with wireless adaptors can communicate with each other and the process controller over the air [2]. Wireless networking offers simple deployment, reconfigurability, scalability, and reduced operational expenditure, and is easier to upgrade than wired solutions. Moreover, it supports flexible communication bandwidth allocation to meet the needs of the control system. Therefore, wireless communications is becoming popular in plants for either reducing the deployment cost to reach the remote nodes in a sparse network or increasing the access capability in a limited space in comparison with cable connectors [3]. Accordingly, a number of wireless industrial communication protocols have been standardized, such as ISA100.11a [4] and WirelessHART [5].

Despite these advantages over their wired peers, the adoption rate of wireless networking has been slow. One popular concern is that the stochastic nature and the less than 100 % reliability of wireless links would impair the control performance [6]. A typical industrial plant is normally built with steel beams and concrete walls and it houses numerous bulky metallic machines, rails and piles of products that make it hard to establish a line-of-sight link between two nodes that need to communicate. The radio signal experiences significant attenuation as it propagates in such a harsh environment. Besides the intrinsic propagation loss, strong co-channel interference is another issue as wireless field instruments, such as Wi-Fi and ZigBee devices, operate in unlicensed spectrum bands, e.g., the 2.4 GHz industrial, scientific and medical (ISM) radio band, and compete for the same scarce spectrum. A number of field studies have been done to verify these concerns. Remley et al. carried out RF channel measurements in industrial plants and reported that the unique propagation features and radio spectrum activities are strongly shaped by the plant architecture and production schedule [7]. Tanghe et al. proposed a channel model for large-scale and temporal fading in industrial indoor environments based on their RF measurement work [8]. The majority of the existing work is still focused on evaluating the wireless channel effects using conventional network performance metrics, such as bit error rate and network throughput. For the plant owners, the real concern is how well the controller behaves when wireless communications are introduced to replace wired connections as well as the installation and operation cost of wireless networks. Therefore, an evaluation of wireless channel effects on the controller performance is sorely needed in order to promote the use of wireless technologies in industrial process control. Currently, this is still an open problem.

In this paper, we study how the control performance is affected by transmissions through wireless links, which are adversely affected by severe propagation loss in harsh industrial environments, co-channel interference, and unintended interference from other devices. These phenomena may result in significant and possibly bursty packet loss, which prevents the controller from tracking the critical performance metrics of the process under control and responding appropriately. We select a chemical process plant as the control process model and identify its communications requirements of connecting various field instruments with the controller through wireless links. We propose two wireless channel models to characterize packet loss patterns in the sensing and actuation links. The process model and the channel model are co-simulated to evaluate the impact of different types of wireless packet loss models on the control performance in various plant operations, such as setpoint change and disturbed operations. Based upon the results, we discuss the adoption of different wireless technologies in process control.

The remainder of the paper is organized as follows. In Section II, the studied process control model is introduced. Two types of wireless channel models are proposed in Section III. The effects of wireless transmissions on control performance are evaluated in Section IV in three different operational scenarios. Finally, we conclude the paper in Section V and discuss possible solutions to improve wireless links in support of control performance.

II. Industrial Process Control Model

We select the Tennessee Eastman Challenge Model (TE) as the model for industrial process control in this paper. The TE process model was first proposed as a simulated chemical plant by Downs and Vogel in 1993 [9]. We chose the TE model for a number of reasons. First, it is a well-known, real-world simulated chemical process model that has many characteristics of a typical dynamic process control study, such as centralized control, networked sensors and actuators, multi-variable optimization, and performance metrics (mainly from the cost perspective) for scenarios with changeable setpoints. The field instruments, being distributed over the plant, need to communicate with the controller over wired or wireless links. Second, the TE model is open-loop unstable, which makes it necessary to periodically update the process variables through the communications links. The adverse effects of the wireless links, in terms of loss or delayed delivery of control data, can significantly degrade the control performance, workplace safety, and economic sustainability. Third, the simulations of the TE process have been well developed so that we can focus on the communications modeling aspect by reusing an existing plant simulation model.

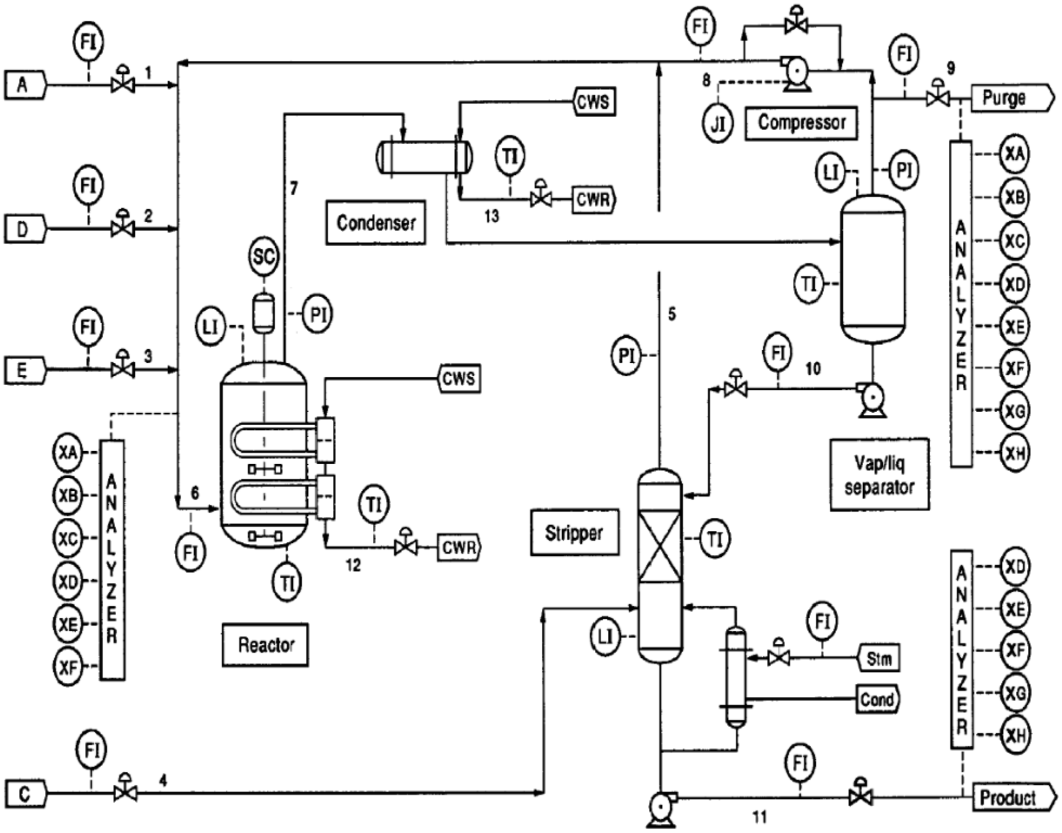


Figure 1. Tennessee Eastman process control problem [9]

The TE plant, shown in Figure 1, is designed for producing two liquid products, G and H, from four gaseous reactant inputs, denoted by A, C, D and E. At the same time, two gaseous byproducts, B and F, are also generated within the process. Note that B, F, G, and H are not explicitly shown in the figure. And instead of revealing the actual chemical process in the plant, generic identifiers are used to represent the substances. The total process is irreversible and divided into five operation stages including a reactor, a product condenser, a vapor-liquid separator, a product stripper, and a recycle compressor. The details of the TE process are described in [9].

For plant process control, the TE model provides a number of measurable process variables (XMEAS) and manipulated variables (XMV) for the controller to probe the health of the process and adjust the production according to the programmed setpoints. The forty-one XMEAS variables are of various types including feed flow rate, container status metric (e.g., temperature, pressure and liquid level indicators), and chemical composition metrics at different process steps. The twelve XMV variables, on the other hand, deal with valve control, temperature control and feed/purge control. The process has a total of six operation modes which control the G/H mass ratio (i.e., XMEAS 40 and XMEAS 41 of stream 11) and the production rate from the stripper underflow (i.e., XMEAS 17 through stream 11). In our study, the primary use case is Mode 1, which is also called the base case.

We choose the decentralized TE controller model proposed by N. Ricker [10] with the heat and material balance data for Mode 1 case in [9] due to its multi-loop distributed control architecture and its wide acceptance as the foundation for viable advanced controller design. In the rest of this paper, whenever we mention the TE process model or the TE model, we mean the TE simulated plant model combined with Ricker's controller model.

III. Communications Channel Model

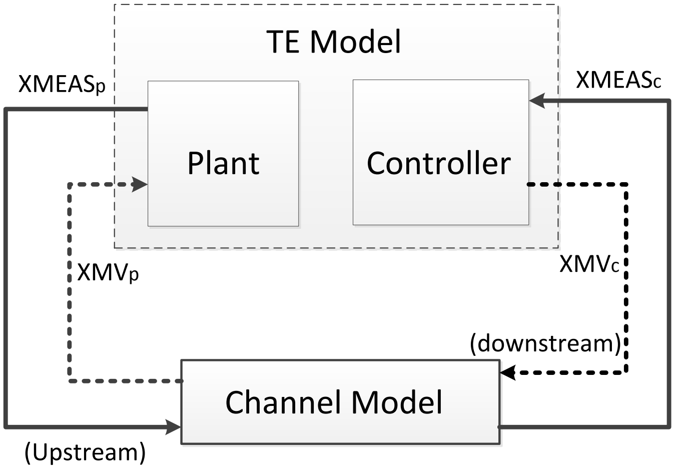


Figure 2. Integrated TE model with communications channel model

In the TE process model, there are two types of communications links depending on the transmission direction. In the upstream links, XMEAS variables, e.g., temperature, pressure and flow rate, acquired from field sensors are transmitted to the controller as shown in Fig. 2. The downstream links, on the other hand, carry the control commands in terms of updates of XMV variables to the field actuation devices. Individual XMEAS and XMV variables will be updated once every T second. In this paper, T is set to 1.8 seconds, consistent with Ricker's Simulink settings [11]. It is assumed that each update will be packed into a separate data packet containing a double variable plus the sampled timestamp. If a data packet gets lost in the communications channel, the receiver will treat that process variable unchanged in the current update and keep using the previous value. Therefore, when wireless communications is used, the packet loss in the wireless channel will have an impact on the process control performance.

The updates through wireless links in both directions are modeled by the following equations,

$$XMEAS_C(n+1) = XMEAS_P(n+1) * \big(1 - E(n+1)\big) + XMEAS_C(n) * E(n+1) \quad (1)$$

$$XMV_P(n+1) = XMV_C(n+1) * \big(1 - E(n+1)\big) + XMV_P(n) * E(n+1) \quad (2)$$

where the subscript C or P for each process variable denotes whether the variable is associated with the controller or the field instrument in the plant, respectively. $E(n)$ is the indicator random variable for the event that a packet loss occurs at the n-th update through the wireless channel. . $E(n)$ is equal to 0 when the packet reaches the destination without error; it is equal to 1 otherwise.

In this paper, we introduce two statistical models to characterize the randomness of the packet loss caused by the wireless channel, namely, an independent and identically distributed (IID) packet loss model and the two-state Gilbert-Elliot (GE) channel model.

A. IID Channel Model

In the IID model, each wireless transmission of a process variable is statistically independent of all others and the probability of a packet not going through is the same at all times. Specifically, the random variables E(n), n = 1, 2, 3, …, are statistically independent and they all have the following probability distribution:

$$\begin{aligned} P\{E(n) = 1\} &= P_{e,iid} \\ P\{E(n) = 0\} &= 1 - P_{e,iid} \end{aligned} . \tag{3}$$

A larger $P_{e,iid}$ indicates a worse wireless channel so that packets are more likely to get impaired and dropped, which forces the controller to take more time to acquire the process status and respond to any disturbances.

B. Gilbert-Elliott (GE) Channel Model

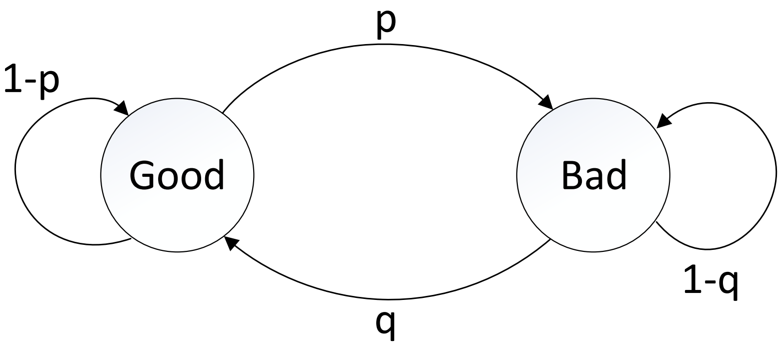


Figure 3. The two-state GE channel model

The GE model is appropriate for modelling bursty losses in wireless links [12-14]. As shown in Fig. 3, the GE model has two states, “good” and “bad”, with $P_{e,G}$ and $P_{e,B}$ denoting the packet error rate (PER) associated with the good and the bad states, respectively. For any two consecutive observation steps, the channel can stay in the same state or jump from one state to the other according to the transition probabilities, p and q, which characterize the burstiness of the good and bad channel conditions. Since the GE model is mathematically a two-state Markov chain, its stationary distribution of channel states, (π_G, π_B), can be calculated by the following equations,

$$\begin{bmatrix} \pi_G \\ \pi_B \end{bmatrix} = \begin{bmatrix} 1-p & q \\ p & 1-q \end{bmatrix} \times \begin{bmatrix} \pi_G \\ \pi_B \end{bmatrix}, \tag{4}$$

$$\pi_G + \pi_B = 1, \tag{5}$$

whose solution is (π_G, π_B)= $(\frac{q}{p+q}, \frac{p}{p+q})$.

The average PER of the GE model is obtained by

$$P_{e,GE} = P_{e,G} * \pi_G + P_{e,B} * \pi_B = \frac{P_{e,G}*q+P_{e,B}*p}{p+q}. \qquad (6)$$

Note that the IID model is a special case of the GE model with $P_{e,G} = P_{e,B} = P_{e,iid}$,.

For the rest of this paper we assume that $P_{e,G} = 0$ and $P_{e,B} = 1$ in the GE model. In other words, the good channel, or the "all-pass" channel, allows the packet to pass through the wireless link without any errors so that $E(n) = 0$. On the contrary, the bad channel totally blocks the packet transmission and results in the packet being dropped, i.e., $E(n) = 1$. Therefore, the temporal dynamics of whether packets go through or get dropped in the GE model are governed by the following equations:

$$\begin{aligned} P\{E(n+1) = 1|E(n) = 0\} &= p \\ P\{E(n+1) = 0|E(n) = 0\} &= 1-p \\ P\{E(n+1) = 0|E(n) = 1\} &= q \\ P\{E(n+1) = 1|E(n) = 1\} &= 1-q. \end{aligned} \qquad (7)$$

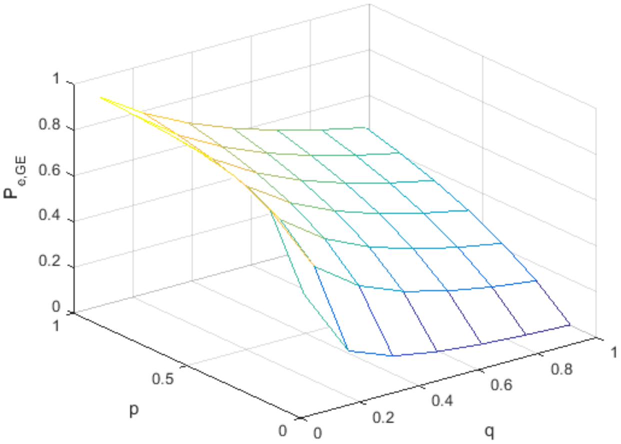


Figure 4. Average PER under different p and q values in GE model ($P_{e,G} = 0$, $P_{e,B} = 1$)

The average PER of (6) can be simplified as

$$P_{e,GE} = 0 * \pi_G + 1 * \pi_B = \frac{p}{p+q}. \qquad (8)$$

The cause of packet loss in wireless channel ranges from strong co-channel interference to overloaded network device in which packets are delayed so much by the device that they are discarded. As shown in Fig. 4, the GE model depicts the impacts of the wireless channel on the transmission with more details than the IID model does. A single $P_{e,GE}$ value may be associated with multiple (p, q) pairs as illustrated in (8). The average run-length for the good and bad states, i.e. the average number of successive number of times the channel stays in the good and bad states turns out to be 1/p and 1/q, respectively. Table 1 illustrates some examples of channel statistics in the GE model.

Table 1. Examples of statistics in GE model (T = 1.8 sec)

p	q	Average PER ($P_{e,GE}$)	Average sojourn time in the good channel (T/p, unit: sec)	Average sojourn time in the bad channel (T/q, unit: sec)
0.10	0.10	0.5	18	18
0.10	0.50	0.1667	18	3.6
0.10	0.90	0.1	18	2
0.50	0.10	0.8333	3.6	18
0.50	0.50	0.5	3.6	3.6
0.50	0.90	0.3571	3.6	2
0.90	0.10	0.9	2	18
0.90	0.50	0.6429	2	3.6
0.90	0.90	0.5	2	2

We assume the GE channel models for transmission of various XMEAS or XMV variables are statistically independent of each other but they all have the same p and q values for the state transition probabilities. When the GE channel is in the bad state, the controller will use the last XMEAS value available to it. By varying (p, q), we can evaluate the effects of the wireless channel model on the communications performance and then extend the discussion to the control performance.

IV. Evaluation of the Wireless Channel Effects

The main control objective of the TE plant is to maintain process variables within prescribed tolerances. When wireless technology is used to communicate the XMEAS and XMV variables, we need to determine whether the control performance would degrade compared with the baseline case of using near perfect wired communications. The major control performance metrics to be used in such a comparison include production flow rate, product mole fractions, and reactor pressure.

We implemented the TE plant model and Ricker's controller design in a C++ simulator along with the two channel models described earlier. The evaluation is performed in three major operation scenarios: fixed optimal setpoint operation, online changed setpoint operation and disturbance-enabled operation. The aforementioned IID and GE channel models are used in the fixed setpoint case so that the sensitivity of the controller to the average PER and channel burstiness is evaluated. Our results for the first scenario indicate that channel burstiness has a negative impact on the control performance, given the same average PER as in the IID model. Therefore, in the following scenarios, the discussions are focused on the control performance variation with the average PER set to the $P_{e,iid}$ value in the IID model.

A. Fixed Setpoint Operation with the IID Channel Model

We first study wireless channel impact on the TE process operating at the optimal setpoints in Mode 1. To assess the impact of wireless packet loss, we select different values of $P_{e,iid}$ in our simulations. In each simulation run, the same value of $P_{e,iid}$ is used in the model for every wireless link between a field instrument and its associated gateway. The gateway is assumed to be connected to the controller without causing any further transmission delays or error. After initializing the plant with the optimal setpoint values from Tables 1 and 3 in [9], each simulation scenario is run for 72 hours of plant operation. Even though every XMEAS and XMV variable gets updated and transmitted once every 1.8 seconds, we record these variables once every 36 seconds (i.e., one out of every 20 samples) for the purposes of analyzing and plotting various performance metrics of the process control problem. We run each simulation scenario once assuming wireless channels are used and once assuming wired channels as the baseline. If any violation of the plant constraints occurs, e.g., the reactor pressure exceeding the prescribed limit, the simulator will automatically pause and record the plant shutdown event in the simulation log.

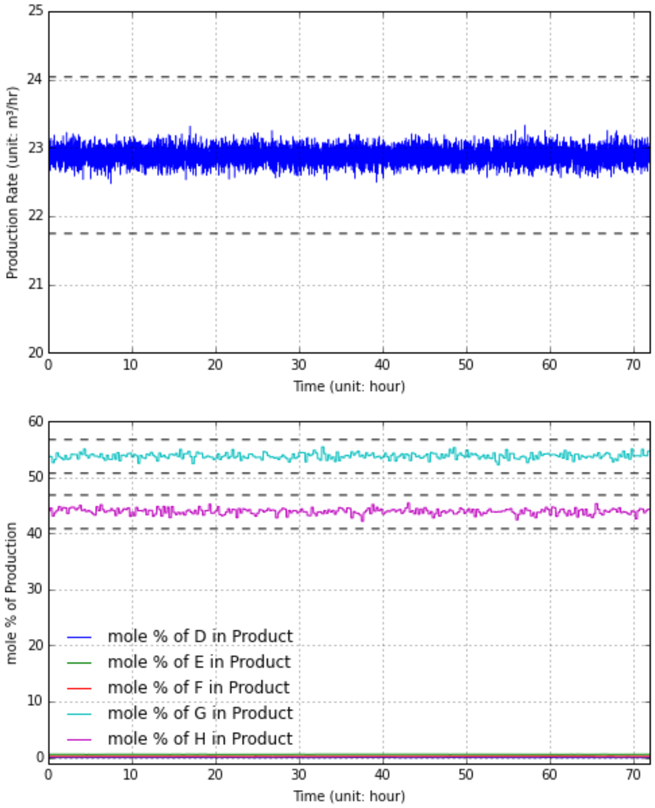


Figure 5. Production rate and product mole fractions in fixed setpoint operation using an IID channel model with ($P_{e,iid} = 0.6$)

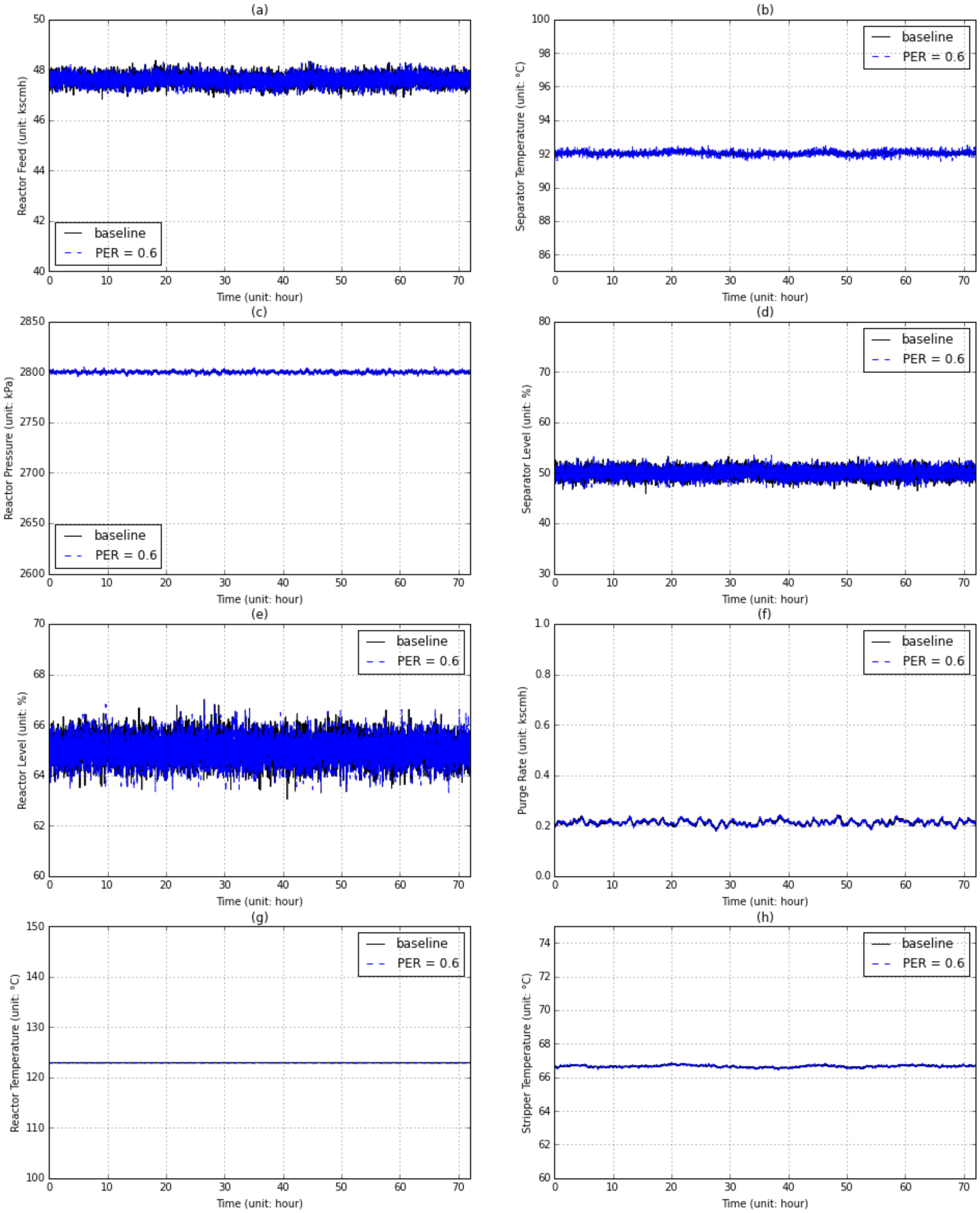


Figure 6. Selected process variables in fixed setpoint operation using IID channel model with ($P_{e,iid} = 0.6$)

The production rate for the plant products should be kept within prescribed limits as well. For example, the stripper underflow (XMEAS 17 in stream 11), should be kept around the optimal setpoint of 22.848 m^3h^{-1}. Meanwhile, the rate variation is expected to remain within 5 % of the setpoint. Besides, as Mode 1 (base case) aims to produce G and H in equal amounts, the mole fractions of G (XMEAS 40) and H (XMEAS 41) in stream 11 should, respectively, be kept at the suggested setpoints of 53.724 % and 43.828± 5 *mol* %. As suggested by [15], the process control works as expected even when a packet loss rate of up to 50-60 % is experienced. Fig. 5 illustrates the variations of the production rate and mol % of the product over a 72-hour period under an IID wireless channel model with $P_{e,iid} = 0.6$. It is observed that the production rates and mole fractions of products G and H fall within the required reliability range. The mole fractions of the other chemicals contained in the under flow, i.e., D, E and F, are negligible after the processing in the separator and the stripper.

Fig. 6 provides more details on the 72-hour plant operation simulation run. When wireless links with ($\mathrm{P_{e,iid}} = 0.6$) are used, as suggested by [15], the TE process maintains similar performance as in the baseline case. This is mainly due to the fact that Ricker's controller design has already incorporated sufficient redundancy to guard against potential data delays/losses. The process update setting of 1.8 seconds is fast enough to detect the slow chemical process variations even if a number of packets are lost. The controller can still rely on the remaining successful updates to avoid missing the important state changes in the plant.

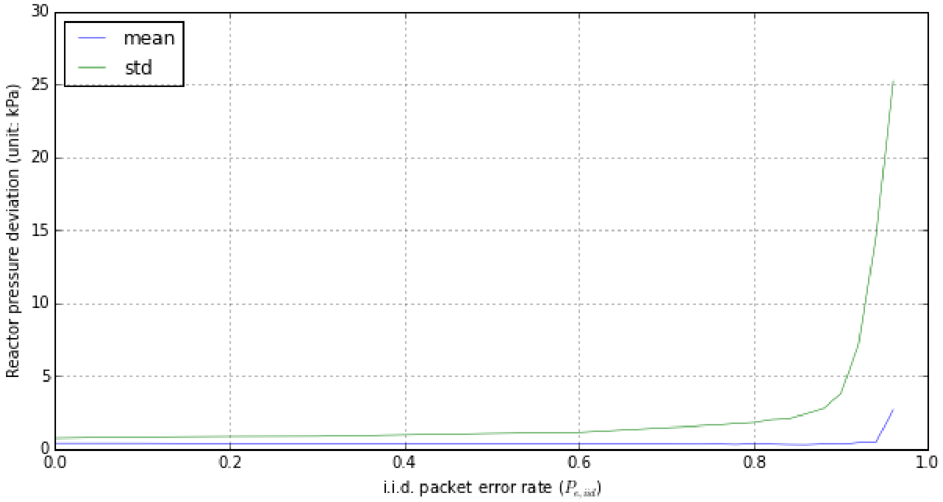


Figure 7. Statistics variation of reaction pressure deviation from the setpoint under different $\mathbf{P_{e,iid}}$

To probe for the limits of the controller in use, we investigate the control performance over a wider PER range. We select the reactor pressure as the performance metric, because it is particularly vulnerable to imperfect control command communications. At the controller, reactor pressure is intended to be driven as high as possible because the reaction efficiency improves as reactor pressure increases [16]. However, the TE process will shut down the plant for safety if the reactor pressure exceeds the safety threshold of 3000 kPa. Therefore, the optimal setpoint of reactor pressure is suggested at 2800 kPa in Mode 1 [9]. When wireless communications is used, as the PER increases, the expected length of the interval between two successful updates increases, which prohibits the controller from quickly responding to the deviation of the reactor pressure from the setpoint. Fig. 7 illustrates the mean and standard deviation of pressure from the setpoint. Each point in Figure 7 represents 100 independent simulation runs with random seeds. It is observed that the reactor pressure control deviates more from the setpoint as the communication channel gets less reliable, which may result in a plant shutdown.

B. Fixed Setpoint Operation with the GE Channel Model

We continue with the fixed setpoint operation scenario, but we change the channel model from IID to GE. While in the case of the IID channel model we mainly focused on the probability of packet loss, which is the same as PER, the evaluation in the GE model case will be focused on the impact of the channel burstiness. The channel burstiness is controlled by the values of p and q. As the value of p (q) decreases, the channel becomes more bursty. In a bursty channel with a small q, when the link experiences one bad transmission, it is highly likely to have another bad transmission during the next update, which impairs the control process. We select different (p, q) pairs in the sample space $(0, 1)^2$, while keeping $P_{e,GE} = \frac{p}{p+q}$ constant. We repeat the simulation at each q for 500 times.

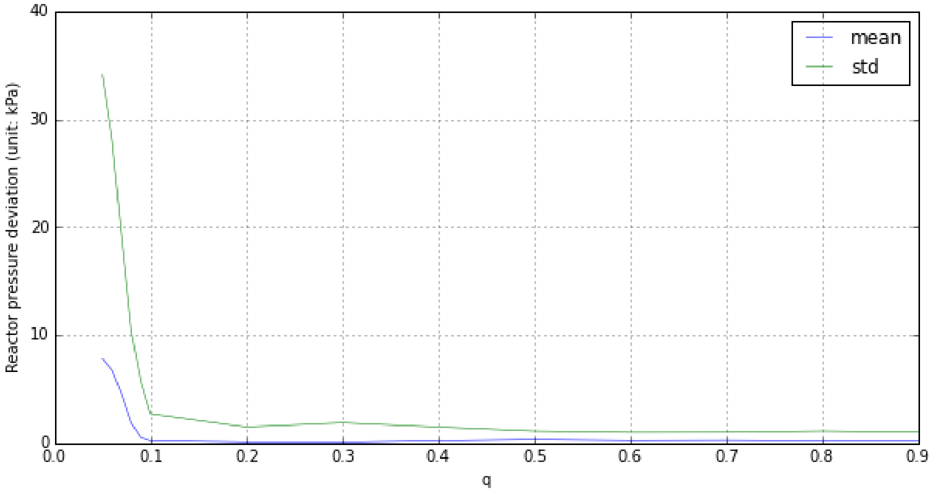


Figure 8. The statistics of reactor pressure deviation from the setpoint vs. q in the GE model with $\mathbf{P_{e,GE} = 0.6}$

Fig. 8 illustrates the mean and standard deviation of pressure deviation as a function of q while $P_{e,GE} = 0.6$. As shown in Table 1, a smaller q leads to a longer interval between successive updates over a wireless link, which reduces the agility of the controller and postpones the manipulation effort. As it can be seen from Figure 7, when the average burst duration for the bad channel is longer than 18 seconds (q<0.1), the TE controller quickly loses pace and deviates away from the desired setpoint. Since the transmission over the wireless channel starts at the beginning of the simulation, it is of interest to determine how long the plant continues to operate until it shuts down.

Fig. 9 illustrates the cumulative distribution function (CDF) of the plant survival time for different q at $P_{e,GE} = 0.6$. Just as there is a significant deviation of the reactor pressure when q<0.1, the plant shuts down rapidly within a few hours. The smaller q is, the faster the shutdown happens.

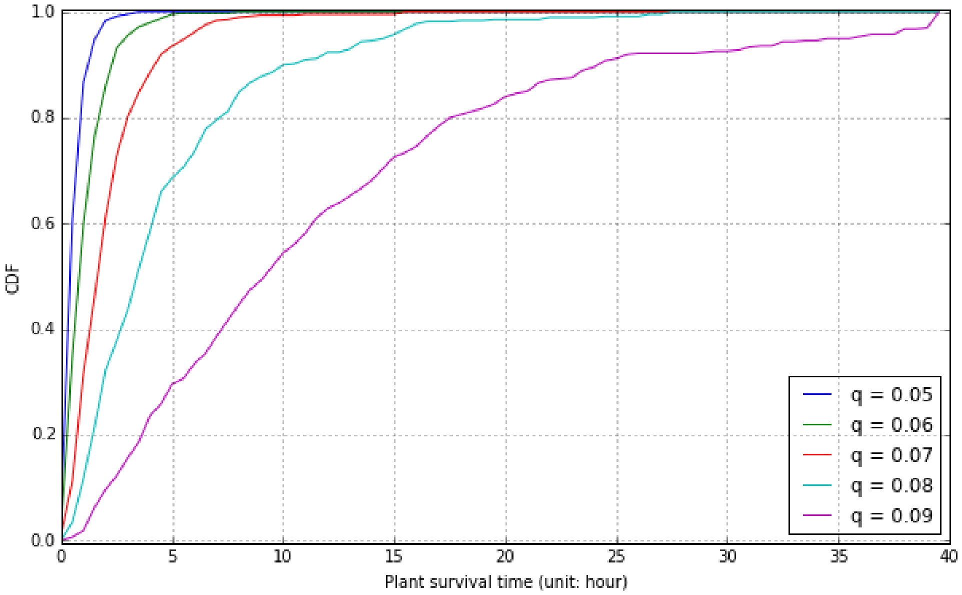


Figure 9. The CDF of plant operation time under different q in the GE model with $P_{e,GE} = 0.6$

C. Changed Setpoint Operation with the IID Channel Model

When a setpoint is intentionally changed during the operation of the plant, the control strategy is designed to manipulate the process to transition to the new stable state gracefully. There are many setpoints that can be changed in the TE model. We study changing the reactor pressure setpoint consistent with previous studies presented earlier in this section. The setpoint for the reactor pressure is tuned from the original value of 2800 kPa to 2500 kPa while other setpoints stay unchanged. The update rate of once every 1.8 seconds is also unchanged in the transition.

As shown in Fig. 10(c), the controller takes multiple discrete time steps to ramp the reactor pressure down, and one undershoot is observed which is due to the control strategy. Similarly, the other process variables experience adjustments and converge to the new stable state. The total adjustment period lasts around 15~20 hours in the simulation. Under the same controller, the control performance with an IID channel model with $P_{e,iid} = 0.6$ in use is comparable with the baseline case of using wired links. We note that the relative difference between any pair of time sequences, one pair for each key performance metric illustrated in Fig. 10, is smaller than 1 % at any time in the simulation.

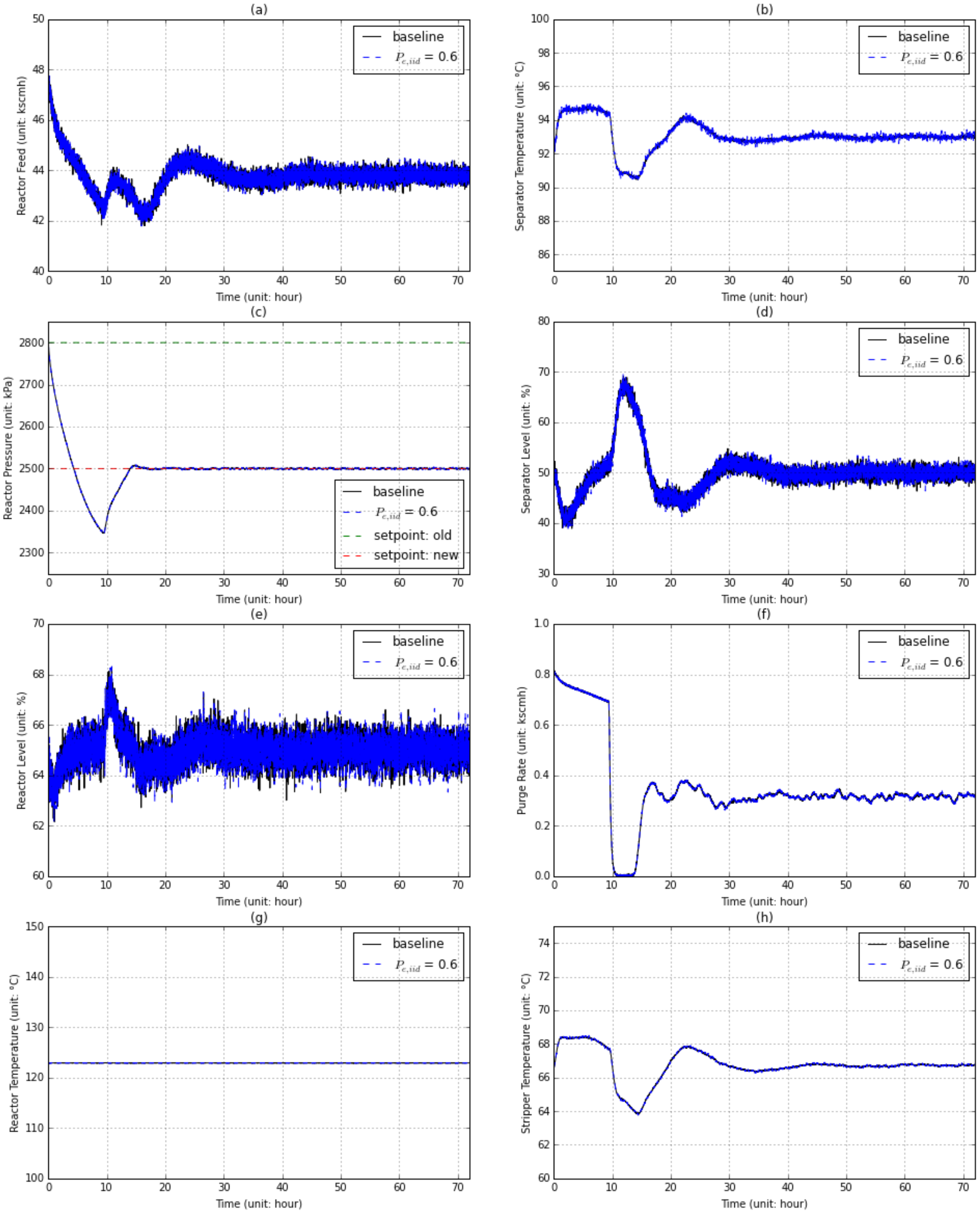


Figure 10. The effects of a change in the reactor pressure setpoint on select process variables using the IID channel model with ($P_{e,iid} = 0.6$)

D. Disturbed Operation with the IID Channel Model

Downs and Vogel [9] suggest 20 different disturbances in the TE model to test the controller performance. We simulate one of their disturbed operation scenarios to evaluate the control performance with wired and wireless links in use.

Figures 11 and 12 illustrate the process performance when random disturbance (IDV 8 in Table 8 [9]) is enabled in the A, B and C feed composition (stream 4). The performance of the controller is excellent in both the baseline links and the wireless IID channel (with $P_{e,iid} = 0.6$). The production rate and the mole fractions of the products are maintained within the specified bounds as shown in Fig. 11. The temperature controller keeps the reactor temperature almost constant at the setpoint even under the disturbance (as shown in Fig. 12(g)), and it also keeps the temperature variations at the separator and stripper (as shown in Fig. 12(b) and 12(h), respectively) at a low frequency (less than 8~10 h^{-1}) although they vary significantly compared with the scenario without the disturbance as shown in Fig. 6. During the whole operation, the controller performs the same whether wireless or wired links are used for communications, which suggests that wireless links can support robust process control even under disturbances.

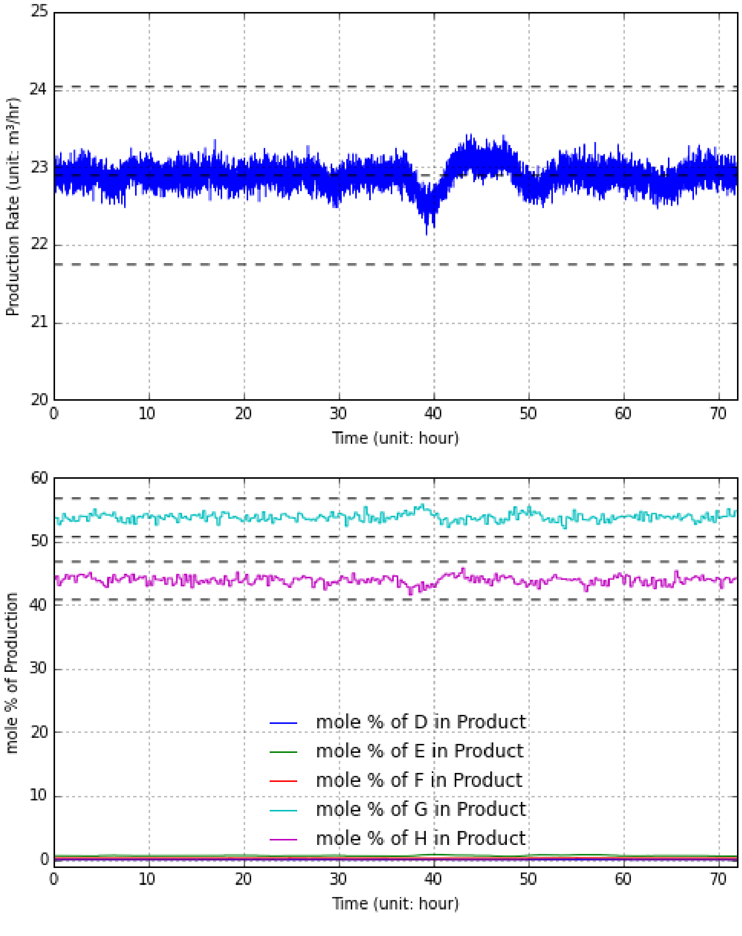


Figure 11. Production rate and product mole fractions using IID model in disturbed operation ($P_{e,iid} = 0.6$, IDV 8 enabled)

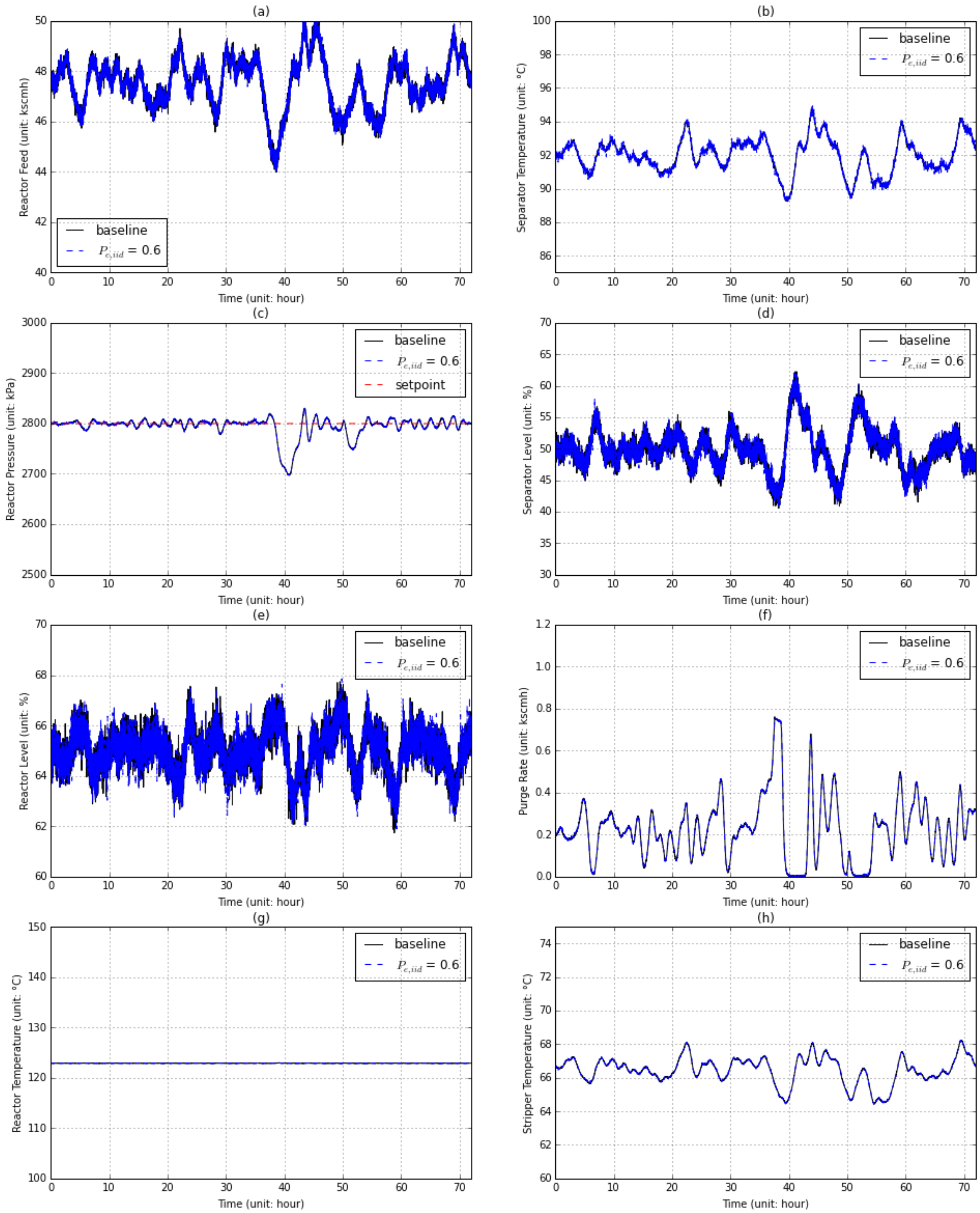


Figure 12. Selected process variables using IID model in disturbed operation ($P_{e,iid} = 0.6$, IDV 8 enabled)

V. Conclusions

In this paper we have evaluated the effects of using wireless communications, mainly the random packet loss, on the industrial process control performance in a simulated chemical process model. Two wireless channel models have been studied in conjunction with three major process operation scenarios. The results indicate that 1) different wireless channels have different effects on the control performance; 2) wireless channels at normal packet loss levels in an industrial environment can support the controller working in fixed setpoint, changed setpoint and the cases where there is a disturbance; and 3) when the wireless links are severely impaired, the controller suffers from large packet loss or long delay, which drives the control process off track and it may cause the plant to shut down. Therefore, it is important to have a good understanding of the RF propagation environment in a given plant before using wireless technology in control operations. Nevertheless, the emerging wireless technologies for industrial control applications can meet the control requirements with careful network provisioning and configuration.

The ISA 100.11a standard provides one viable solution to build a wireless network to support industrial process control systems. Consider the TE process control problem as an example:

1. The ISA100.11a standard provides programmable time slots and a repeatable frame structure for periodic process variable updates. For the TE model, with the time slot duration set to 10 milliseconds, a frame containing 180 time slots, corresponding to one update every 1.8 s, can easily serve the control update task by accommodating 53 direct communications links between the gateway and the field instruments by allocating one time slot to each update packet. The remaining time slots can be used for packet retransmissions, which further improves the success of the process update operation.
2. Frequency hopping employed in the ISA100.11a standard can greatly improve the wireless link performance in the plant environment under severe RF interference conditions. As there are a total of 16 non-overlapping wireless channels available in the 2.4 GHz ISM frequency band, per-slot channel hopping prevents a given link from always suffering from strong interference in the same channel. The ISA100.11a standard also supports black listing of channels that are detected to be suffering from being in bad state for a long period of time.
3. The PHY layer protocol of the ISA100.11a standard is based on the IEEE 802.15.4 standard, which uses the direct sequence spread spectrum (DSSS) technology to reduce the noise/interference in the received signal for better link performance. Moreover, ISA100.11a increases the maximum transmission power to 10 dBm in comparison with the standard IEEE 802.15.4 radios. This improves the quality of the received radio, which would prove useful in the harsh industrial plant RF propagation environment.

In future work we will study the implementation of an ISA100.11a network for the TE process problem based on the lessons learned from this paper. A joint modeling and co-simulation of the process control problem and the wireless network behavior will be studied. In addition, we will evaluate various techniques, such as multi-path routing, multi-channel hopping, and scheduling for prioritized emergency control messaging, for improving wireless link performance in support of industrial control applications.

DISCLAIMER

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

REFERENCES

[1] J. H. Lee and J. M. Lee, “Progress and Challenges in Control of Chemical Processes,” *Annu. Rev. Chem. Biomol. Eng.*, vol. 5, no. 1, pp. 383–404, 2014.

[2] A. Kumar Somappa, K. Øvsthus, and L. M. Kristensen, “An Industrial Perspective on Wireless Sensor Networks: A Survey of Requirements, Protocols, and Challenges,” *IEEE Commun. Surv. Tutor.*, vol. 16, no. 3, pp. 1391–1412, 2014.

[3] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. M. Leung, “Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT,” *IEEE Access*, vol. 3, pp. 622–637, 2015.

[4] “Wireless Systems for Industrial Automation: Process Control and Related Applications”, ISA-100.11a-2009 Standard, 2009.

[5] IEC 62591 Ed. 1.0 b:2010, “Industrial Communication Networks—Wireless Communication Network and Communication Profiles—WirelessHART™,” 2010.

[6] A. Kumar Somappa, K. Øvsthus, and L. M. Kristensen, “An Industrial Perspective on Wireless Sensor Networks: A Survey of Requirements, Protocols, and Challenges,” *IEEE Commun. Surv. Tutor.*, vol. 16, no. 3, pp. 1391–1412, 2014.

[7] Kate Remley, et al., “NIST Tests of the Wireless Environment in Automobile Manufacturing Facilities”, NIST Technical Note 1550, 2008.

[8] E. Tanghe, et al., “The Industrial Indoor Channel: Large-Scale and Temporal Fading at 900, 2400, and 5200 MHz”, *IEEE Trans. Wireless Comm.*, vol. 7, no. 7, pp. 2740-2751, Jul. 2008.

[9] J. J. Downs and E. F. Vogel, “A Plant-wide Industrial Process Control Problem”, *Comput. Chem. Engng.*, vol. 17, no. 3, pp. 245-255, 1993.

[10] N. L. Ricker, “Decentralized Control of the Tennessee Eastman Challenge Process”, *J. Proc. Cont*. vol. 6, no. 4, pp. 205-221, 1996.

[11] N. Lawrence Ricker. (2002, December) New Simulink models of two decentralized control strategies. [Online]. http://depts.washington.edu/control/LARRY/TE/download.html#Multiloop

[12] E. N. Gilbert, “Capacity of a Burst-Noise Channel”, *Bell Syst. Tech. J.*, vol. 39, pp. 1253-1265, Sept. 1960.

[13] E. O. Elliott, “Estimates of Error Rates for Codes on Burst-Noise Channels”, *Bell Syst. Tech. J.*, vol. 42, pp. 1977-11997, Sept. 1963.

[14] G. Haßlinger and O. Hohlfeld, "The Gilbert-Elliott Model for Packet Loss in Real Time Services on the Internet”, *GI/ITG MMB'08*, 2008

[15] Emerson Process Management, “System Engineering Guideline - IEC 62591 WirelessHART”, Rev. 04, May 2014.

[16] Alvaro Cardenas et al., "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response," in *ASIACCS 2011*, Hong Kong, China, 2011.

Integrating Top-down and Bottom-up Cybersecurity Guidance using XML

Joshua Lubell
National Institute of Standards and Technology

Abstract

This paper describes a markup-based approach for synthesizing disparate information sources and discusses a software implementation of the approach. The implementation makes it easier for people to use two complementary, but differently structured, guidance specifications together: the (top-down) Cybersecurity Framework and the (bottom-up) National Institute of Standards and Technology Special Publication 800-53 security control catalog. An example scenario demonstrates how the software implementation can help a security professional select the appropriate safeguards for restricting unauthorized access to an Industrial Control System. The implementation and example show the benefits of this approach and suggest its potential application to disciplines other than cybersecurity.

Table of Contents

1. Introduction

The Cybersecurity Framework [CSF] and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 [SP800-53] are complementary cybersecurity guidance specifications. The Cybersecurity Framework helps practitioners raise awareness within an organization and communicate assessments and objectives to stakeholders. SP 800-53 provides a rigorous methodology for tailoring a comprehensive catalog of security controls to meet an organization's risk management needs. The Cybersecurity Framework facilitates top-down decision-making, whereas NIST SP 800-53 enables a more bottom-up approach to managing cyber-risk.

Because the Cybersecurity Framework and NIST SP 800-53 are complementary, using the two together can provide a greater benefit than using either alone. But combining the top-down, mission-focused guidance in the Cybersecurity Framework with the bottom-up risk management guidance in NIST SP 800-53 is a challenge. Markup technologies can synthesize the security guidance from the Cybersecurity Framework and NIST SP 800-53 into a coherent whole.

This paper presents research demonstrating that software implemented entirely in the Extensible Markup Language (XML) [XML] can effectively make it easier for security professionals to use the Cybersecurity

Lubell, Joshua.
"Integrating Top-down and Bottom-up Cybersecurity Guidance using XML."
Paper presented at the Balisage Series on Markup Technologies, Washington, DC, Aug 2-Aug 5, 2016.

Framework and NIST SP 800-53 together. The research also suggests that the approach presented can be successful in solving the more general problem of developing a user interface (UI) to integrate and synthesize information from disparate sources, provided that the quantity of information and number of sources are small enough to not overwhelm limited computational or software development resources. In other words, this approach is intended to enable a developer whose day job does not primarily involve coding to write platform-independent software that is easy and inexpensive to deploy.

The rest of this paper proceeds as follows. Section 2 provides an overview of NIST SP 800-53 and the Cybersecurity Framework. Section 3 presents the technical approach: first in general terms applicable to any scenario involving integration of disparate guidance sources, and then as applied to the implementation discussed in Section 4. Section 4 introduces Baseline Tailor, a software application, implemented using the approach discussed in Section 3, that makes it easier for people to use the Cybersecurity Framework and NIST SP 800-53 security control catalog together. Section 5 presents an example usage scenario demonstrating how Baseline Tailor can help a security professional select the appropriate safeguards for restricting unauthorized access to an Industrial Control System (ICS). Section 6 summarizes some previous third-party research efforts that influenced this work. Section 7 concludes the paper.

2. Background: NIST SP 800-53 and the Cybersecurity Framework

NIST SP 800-53 provides guidance for selecting and tailoring security controls for information systems. The security controls defined in NIST SP 800-53 should be applied as part of a rigorous risk management process. NIST SP 800-53 organizes its catalog of security controls into eighteen families with each family representing a general security topic. A two-character identifier uniquely identifies the family. Each control has zero or more control enhancements, each of which adds additional functionality to or increases the strength of the control. The catalog specifies three security control baselines: for low, moderate, and high impact information systems. NIST recommends the baselines as starting points for security control selection. For example, an organization looking to select security controls for a low impact system (where the consequences of compromised confidentiality, integrity, and availability of information are low) might begin with the controls in the baseline for the low impact level (or more succinctly, the low baseline) and tailor them as appropriate.

Table 1 shows the low, moderate, and high baselines for the first six controls in the Access Control (AC) family. In most cases, the moderate baseline is a superset of the low baseline, and the high baseline is a superset of the moderate baseline. The numbers in parentheses in the two rightmost columns denote control enhancements, which are declarations of security capability to increase the control's functionality and/or strength. For example, AC-2 (1), which identifies control enhancement (1) of AC-2 (Account Management), states a set of capabilities specific to automated system account management. These capabilities enhance the more general capabilities stated for AC-2, which apply to all types of account management. This paper discusses security control AC-2 in further detail in Section 4, where Figure 6 shows AC-2's XML representation in Baseline Tailor, and in the usage scenario in Section 5.

NIST SP 800-53 also contains guidance for creating and documenting overlays to encourage the sharing of best security practices. An overlay is a set of control customizations applicable to a group of organizations with common security requirements. For example, NIST SP 800-82 (Guide to ICS Security) [SP800-82] specifies an overlay for Industrial Control Systems, which are common in the utility, transportation, chemical, pharmaceutical, process, and durable goods manufacturing industries. An ICS is vulnerable to many of the same security threats that affect traditional information systems, yet has unique needs requiring additional guidance beyond that offered by NIST SP 800-53.

The Cybersecurity Framework provides a way for organizations to describe their current security posture and target state, and to communicate and assess progress toward meeting goals. The Cybersecurity

Framework is organized in a hierarchical fashion, which allows for high-level as well as detailed descriptions of security outcomes. It can facilitate communication not only between different categories of stakeholders but also between different levels of management within an organization, for example, between a chief executive and cybersecurity professionals responsible for implementation. In addition, the Cybersecurity Framework links desired security outcomes to specific NIST SP 800-53 security controls, as well as to sections of other standards, guidelines, and best practices offering guidance on how to achieve desired cybersecurity outcomes. This paper focuses specifically on the links to NIST SP 800-53.

Table 1.

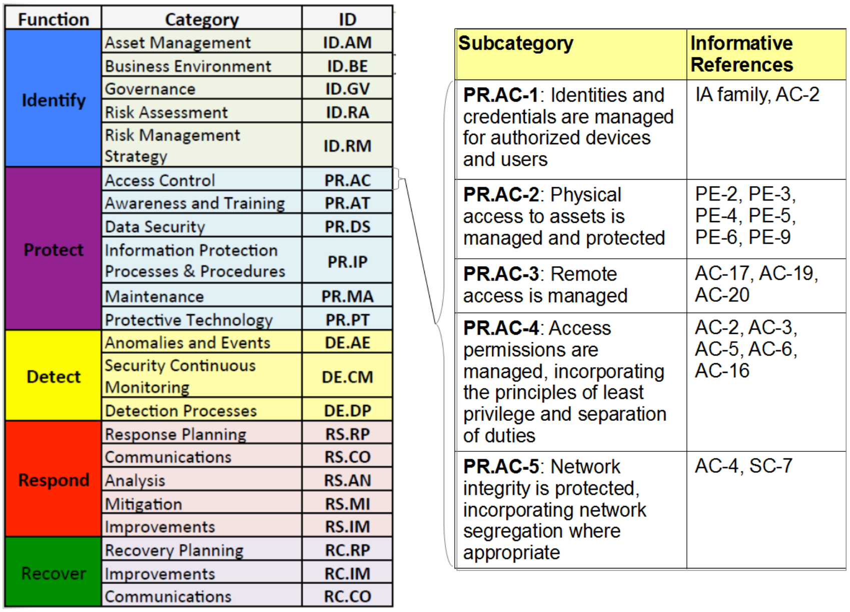
Low, moderate, and high baselines for the first six controls in the Access Control (AC) family.

ID	NAME	LOW	MODERATE	HIGH
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)

A major component of the Cybersecurity Framework is the Framework Core, a taxonomy of cybersecurity outcomes common across critical infrastructure sectors. The highest level of the Framework Core consists of five overarching cybersecurity functions: “Identify”, “Protect”, “Detect”, “Respond”, and “Recover”. Each function has a two-character identifier: ID for “Identify”, PR for “Protect”, DE for “Detect”, RS for “Respond”, and RC for “Recover”. Each function is subdivided into categories, which are high-level outcomes. Each category's identifier consists of its function identifier, followed by a period, followed by two more characters such that the category identifier uniquely identifies the category. Each category in turn contains a set of subcategories, which are specific lower-level outcomes that support the category’s higher-level outcome. Subcategories are identified numerically in a manner similar to that of security controls within a control family. Each subcategory has informative references providing guidance for achieving the subcategory’s outcome, including references to NIST SP 800-53 security control definitions. The NIST SP 800-53 informative references are essential for synthesizing the Cybersecurity Framework and NIST SP 800-53 guidance, as will be shown in Section 4.

Figure 1 shows the Framework Core functions and categories, with the “Protect” function's “Access Control” category (PR.AC) expanded to show all five of its subcategories. The Informative References column on the right only shows references to NIST SP 800-53. References to other standards, guidelines, and best practices are excluded because they are out of scope for this paper. As this column shows, the Cybersecurity Framework is less granular than NIST SP 800-53. References are to controls in their entirety, and do not distinguish between control enhancements or baselines.

Figure 1.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
PR.AC-1: Identities and credentials are managed for authorized devices and users	IA family, AC-2
PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
PR.AC-3: Remote access is managed	AC-17, AC-19, AC-20
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	AC-4, SC-7

Cybersecurity Framework Core with expansion of category PR.AC.

A Framework Profile is a subset of the outcomes in the Framework Core representing either an organization’s current or target security posture. The Cybersecurity Framework is not prescriptive with respect to how an organization should create a Profile, or how much information a Profile should include beyond an enumeration of the Framework Core subcategories it includes. However, the Cybersecurity Framework suggests that an organization consider basing a Profile on business drivers and an assessment of and tolerance for risk. The Baseline Tailor usage scenario discussed in Section 5 involves use of a Framework Profile to support the selection of NIST SP 800-53 security controls. This scenario specifically illustrates how a Framework Profile focusing on category PR.AC (Access Control) can support selection of security control AC-2 (Account Management).

3. An XML-based Integration Approach

For a general integration approach, applicable for other disciplines besides cybersecurity, consider a generic scenario where multiple information sources need to be combined such that the combined information can be efficiently viewed and manipulated using a common UI. These information sources may or may not be structured XML data. For example, they may be in the form of tables in a document, or as spreadsheets. These information sources can be thought of as Small Arcane Nontrivial Datasets [Lubell2014]. Although not large enough to justify a heavyweight, server-based database application, a Small Arcane Nontrivial Dataset is complex enough to benefit from specialized software for manipulation and access, and important enough to justify the development of such software. Let us further assume a requirement that any results of manipulating the data be presented to the user as structured XML. The following general approach for developing such software that meets the aforementioned requirements uses three XML technologies: XForms, Extensible Stylesheet Language Transformations (XSLT), and the XML Path Language (XPath).

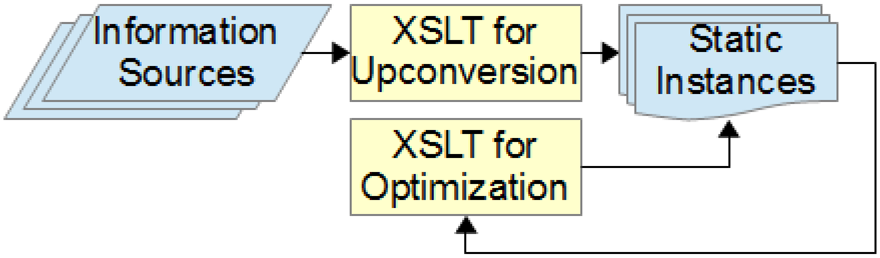
XForms [XForms], an XML application for specifying forms for the Web, is well-suited for implementing UIs for Small Arcane Nontrivial Datasets. XForms adopts the model-view-controller software pattern, making it a good fit for lightweight, data-driven applications. The XForms model consists of a set of instances and a set of bindings. The instances are well-formed XML documents, some static and some dynamic. The bindings define UI constraints, compute dynamic instance data values from other instance data, and manage the display of UI widgets. Because XForms is an XML language, XForms is a good choice for implementations where data is already available as XML, or when XML output is desired. XForms provides a platform-independent set of UI widgets, enabling the same XForms-valid source code to run in multiple browser environments and on multiple operating systems.

Since XForms requires model instances to be well-formed XML, the original information sources may need to be converted to XML from their native formats. XSLT [XSLT] is particularly well-suited for such a task, even if the source data is non-XML or semi-structured as is the case with Small Arcane Nontrivial Datasets that are spreadsheets or tabular data extracted from documents. If the source is poorly structured, a semi-automated approach combining XSLT with hand-editing may be needed. XSLT is also useful for making flat data hierarchical or vice versa. Additionally, XSLT can be used to create multiple alternatively-structured XForms instances in order to speed up UI operations (at the expense of memory requirements — a space-time tradeoff).

XForms and XSLT both depend on XPath [XPath]. XForms uses XPath for bindings within the model as well as for specifying interactions between the UI widgets and the model. XSLT uses the XPath data model and XPath's library of functions and operators.

Figure 2 shows a generic pipeline for producing static XForms model instances from native information sources. The pipeline uses XSLT to up-convert an unstructured or semi-structured information source into a well-formed, well-structured instance. XSLT is also used to create additional static instances optimized for specific UI operations.

Figure 2.



Generic XML transformation pipeline to produce XForms static model instances.

In the event that the native information source is too poorly structured to support transformation without human intervention, the following semi-automated procedure for extracting tabular data from a semi-structured documentary source can be used:

1. If the document is not in an Office Open XML [ISO29500] Spreadsheet (`.xlsx`) format, save it in `.xlsx` form (see Disclaimer).

2. Determine how the information should be represented as structured XML. This is primarily a data modeling exercise.

3. Open up the result in a spreadsheet authoring software application and, using copy/paste, partition the file into separate Office Open XML Spreadsheet documents such that each document contains a simple tabular spreadsheet with no split cells or cells spanning multiple rows or columns.

4. For each tabular spreadsheet document, create a mapping from columns to XML elements and, using the map, convert the spreadsheet to structured XML.

5. Using XSLT, combine the XML documents as desired, and up-convert ill-structured data within cells as required.

4. Baseline Tailor Overview and Implementation

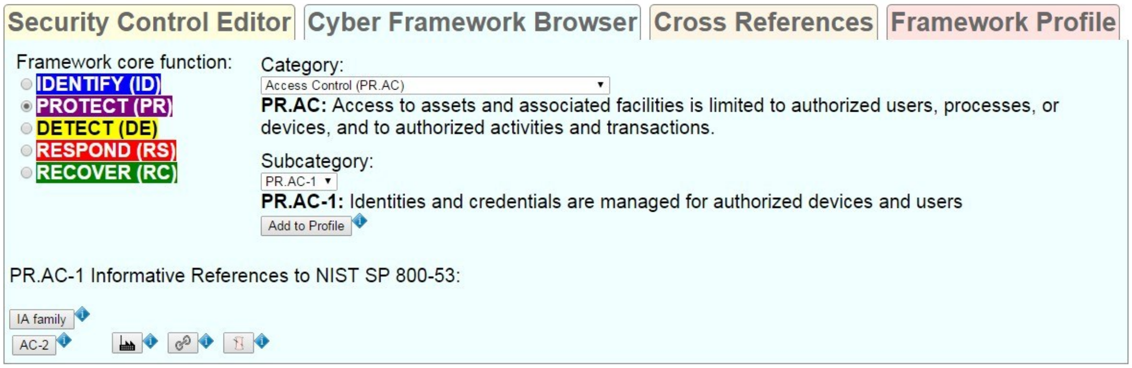
The generic recipe described in the previous section was applied to develop Baseline Tailor, a freely available and open source software tool specifically for users of the Cybersecurity Framework and NIST SP 800-53 security controls. The Baseline Tailor User Guide [Lubell2016] describes this software, and multiple usage scenarios, in detail. [Lubell2015] provides some implementation details, not discussed in this paper, that are specific to Baseline Tailor's UI for tailoring security controls. Section 5 describes a specific Baseline Tailor usage scenario: synthesizing into a coherent whole the security guidance from NIST SP 800-53, the Cybersecurity Framework, and the NIST SP 800-82 ICS overlay. Without Baseline Tailor, an individual wishing to use these specifications together would have to deal with three separate information sources, each organized differently. Baseline Tailor’s UI makes it easier to use the specifications together. Additionally, Baseline Tailor provides new information derived through integrating the disparate information sources – information not obvious from studying each specification in isolation.

A Baseline Tailor user utilizes the Cybersecurity Framework to determine an organization’s desired security posture, and then tailors an appropriate subset of SP 800-53 security controls needed to make that desire a reality. The Baseline Tailor UI lets users see how Cybersecurity Framework core functions, outcomes and SP 800-53 security controls all relate to one another. It also automatically enforces SP 800-53 tailoring rules. Additionally, the UI produces output in XML so results can be fed directly to other software tools to generate reports, share requirements, or establish assurance. [Lubell2016] discusses Baseline Tailor's XML format for tailored controls, UI support for tailoring controls, and automated SP 800-53 enforcement in detail.

The Baseline Tailor UI, shown in Figure 3, has four tabs:

- A Security Control Editor tab for navigating the NIST SP 800-53 security control catalog and tailoring controls.
- A Cyber Framework Browser tab for navigating the Framework Core and modifying a Framework Profile, the active tab in Figure 3.
- A Cross References tab showing all references from the Framework Core to a particular security control.
- A Framework Profile tab for modifying a Framework Profile and showing the currently-selected subset of Framework Core outcomes.

Figure 3.



Security Control Editor | Cyber Framework Browser | Cross References | Framework Profile

Framework core function:
○ IDENTIFY (ID)
● PROTECT (PR)
○ DETECT (DE)
○ RESPOND (RS)
○ RECOVER (RC)

Category:
Access Control (PR.AC) ▼
PR.AC: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Subcategory:
PR.AC-1 ▼
PR.AC-1: Identities and credentials are managed for authorized devices and users
Add to Profile

PR.AC-1 Informative References to NIST SP 800-53:

IA family
AC-2

Cyber Framework Browser tab.

Figure 4 shows the transformation pipeline used to produce the Baseline Tailor XForms static model instances. This pipeline is a specialization of the pipeline in Figure 2. The pipeline transformed the following native information sources, enclosed by a coarsely dashed border in Figure 4:

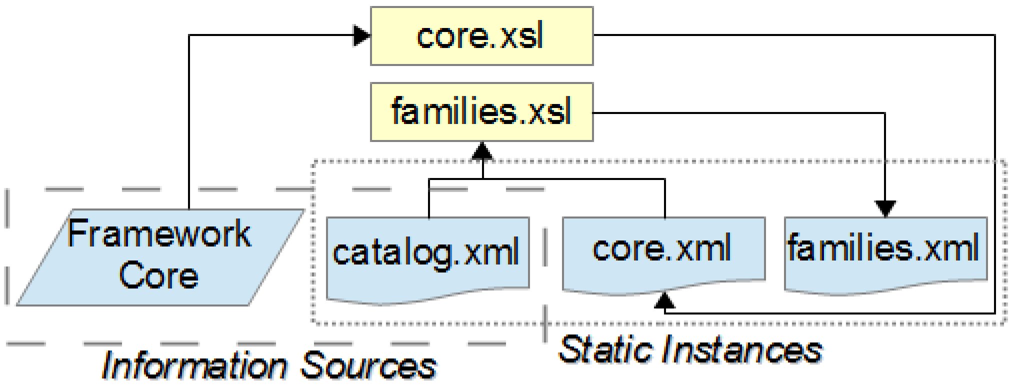
- A tag-delimited tabular representation of the Framework Core, obtained from a Filemaker Pro runtime database (see Disclaimer) available from the Cybersecurity Framework website [CSFTool].

- `catalog.xml`: the structured XML representation of the NIST SP 800-53 security control catalog available from the NIST SP 800-53 database [NVD]. Since the security catalog's native format is structured XML, it is usable as-is as an XForms model instance.[1] Therefore, Figure 4 shows `catalog.xml` as enclosed within both the coarsely-dashed border surrounding the information sources and the finely-dashed border surrounding the XForms static instances. Baseline Tailor uses the data in catalog.xml to generate the portion of the UI in the Security Control Editor tab for tailoring a security control and its control enhancements. Figure 11 shows this portion of the UI when a user has selected security control AC-2 for tailoring.

The XSLT stylesheet `core.xsl` up-converted the semi-structured Framework Core data into a hierarchically structured XForms static instance `core.xml`. Baseline Tailor uses the data in `core.xml` to generate the "Framework core function" radio buttons, "Category" and "Subcategory" drop-down lists, and "Informative References" buttons shown in Figure 3.

The XSLT stylesheet `families.xsl` generated a static instance `families.xml` using the data in `catalog.xml` and `core.xml`. `families.xml` is optimized to facilitate retrieval of security controls belonging to a family, and adds for each security control the identifiers from `core.xml` identifying the Framework Core subcategories that reference the control. The subcategory identifiers are vital to Baseline Tailor for integrating the Cybersecurity Framework and NIST SP 800-53 guidance. Baseline Tailor uses the subcategory information in `families.xml` to generate the information shown in the Cross References tab. Figure 12 shows the Cross References tab after a user has requested the cross references for security control AC-2.

Figure 4.



XML transformation pipeline used to produce Baseline Tailor XForms static model instances.

The XML shown in Figure 5 and Figure 6 illustrates how the Baseline Tailor XForms model represents security controls, subcategories, and their inter-relationships. Figure 5 shows how `core.xml` represents the category PR.AC (shown earlier as a table in Figure 1). Each `category` element has an `id` attribute and contains `subcategory` elements representing the category's subcategories. To reduce Figure 5's verbosity, only the subcategories with informative references to security control AC-2 — PR.AC-1 and PR.AC-4 — are shown in full detail.

[1] Actually, Baseline Tailor does not use the original catalog XML as-is. The original source contains detailed prose text statements from the NIST SP 800-53 Revision 4 document describing each security control in the catalog. Baseline Tailor's UI does not need these descriptions, so they were stripped from Baseline Tailor's `catalog.xml` model instance for efficiency reasons. However, it is fair to say that Baseline Tailor *could* — at least in theory — use the original XML as-is.

Figure 5.

```
<category id="PR.AC">
  <name>Access Control</name>
  <description>Access to assets…</description>
  <subcategory id="PR.AC-1">
    <description>Identities and credentials…</description>
    <sp800-53>
      <control>AC-2</control><family>IA</family>
    </sp800-53>
  </subcategory>
  <subcategory id="PR.AC-2">…</subcategory>
  <subcategory id="PR.AC-3">…</subcategory>
  <subcategory id="PR.AC-4">
    <description>Access permissions are…</description>
    <sp800-53>
      <control>AC-2</control><control>AC-3</control>
      <control>AC-5</control><control>AC-6</control>
      <control>AC-16</control>
    </sp800-53>
  </subcategory>
  <subcategory id="PR.AC-5">…</subcategory>
</category>
```

XML representation of category PR.AC in `core.xml` showing informative references to security control AC-2. Ellipsis symbols indicate content not relevant to the example.

Figure 6 shows how `families.xml` represents security control AC-2. Baseline Tailor uses the `family` element's `name` attribute to populate the UI's “Control family” drop-down list, shown in Figure 9. After the user selects a family from the list, Baseline Tailor uses the `control` element’s `number` attribute and `title` element to populate the UI's Control drop-down list, shown in Figure 10. The `default` element represents a security control's baseline impact level (“1” for low, “2” for moderate, “3” for high, and “4” if the control is not in one of the NIST SP 800-53 baselines). The `priority` element represents a security control's priority code. NIST SP 800-53 recommends that Priority 1 controls should be implemented first, followed by priority 2, and finally priority 3. Baseline tailor uses a control's `default` and `priority` sub-elements, in conjunction with the user's “Baselines” and “Priorities” checkbox selections (as shown in Figure 10), to determine whether to include the control in the “Control” drop-down list.

The control's `subcategory` elements reference all Framework Core subcategories that informatively reference the control. The `number` attributes provide these reverse references. The reverse references to PR.AC-1 and PR.AC-4 correspond to the informative references shown in Figure 5.

Figure 6.

```
<family name="ACCESS CONTROL">
  <control number="AC-1">…</control>
  <control number="AC-2">
    <title>ACCOUNT MANAGEMENT</title>
    <default>1</default>
    <priority>1</priority>
    <subcategory number="PR.AC-1"/>
    <subcategory number="PR.AC-4"/>
    <subcategory number="DE.CM-1"/>
    <subcategory number="DE.CM-3"/>
  </control>
  …
</family>
```

XML representation of “Access Control” family in `families.xml` showing cross references from security control AC-2 to Framework Core subcategories shown. Ellipsis symbols indicate content not relevant to example.

5. Baseline Tailor Usage Scenario

The flowchart in Figure 7 shows a suggested workflow for the Baseline Tailor usage scenario of using a Framework Profile and NIST SP 800-82 to support selection of NIST SP 800-53 security controls. The user begins by creating a Profile containing a set of Framework Core subcategories needed to meet a cybersecurity requirement. Next, the user considers each of the Profile’s informative references. For each security control referenced, the user performs the following actions to determine how critical the security control is to achieving the Profile’s outcomes:

- Checks how many of the Profile’s subcategories reference the security control.

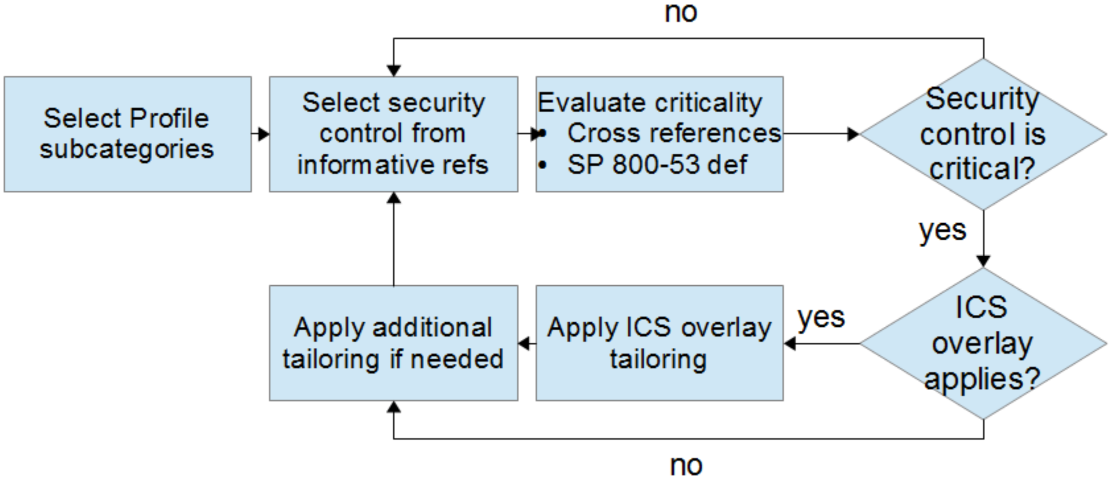
- Views the security control’s NIST SP 800-53 online database definition to determine relevance.

If the user deems the security control to be critical for meeting the cybersecurity requirement, the user then proceeds to tailor the security control. The user may apply the NIST SP 800-82 ICS overlay tailoring guidance, if applicable, as a starting point.

As a concrete example of the workflow in Figure 7, suppose a cybersecurity analyst wants to protect an ICS. The analyst decides to use Baseline Tailor to help determine which security controls should be selected and tailored for implementation. The analyst begins by choosing the “Protect” (PR) core function and “Access Control” (PR.AC) category in the Cyber Framework Browser tab (as shown in Figure 3). Using the Subcategory drop-down list, the analyst next looks at PR.AC’s five subcategories and decides to create a Profile containing all of them. To do so, the analyst switches to the Framework Profile tab and makes the checkbox selections shown in Figure 8. Baseline Tailor creates a simple XML representation of the Profile on the fly. The Profile, a dynamic XForms model instance, is used to generate (also on the fly) XML output shown in non-editable text field at the bottom of the figure. This XML may be copy- pasted into a third-party XML authoring tool.[2]

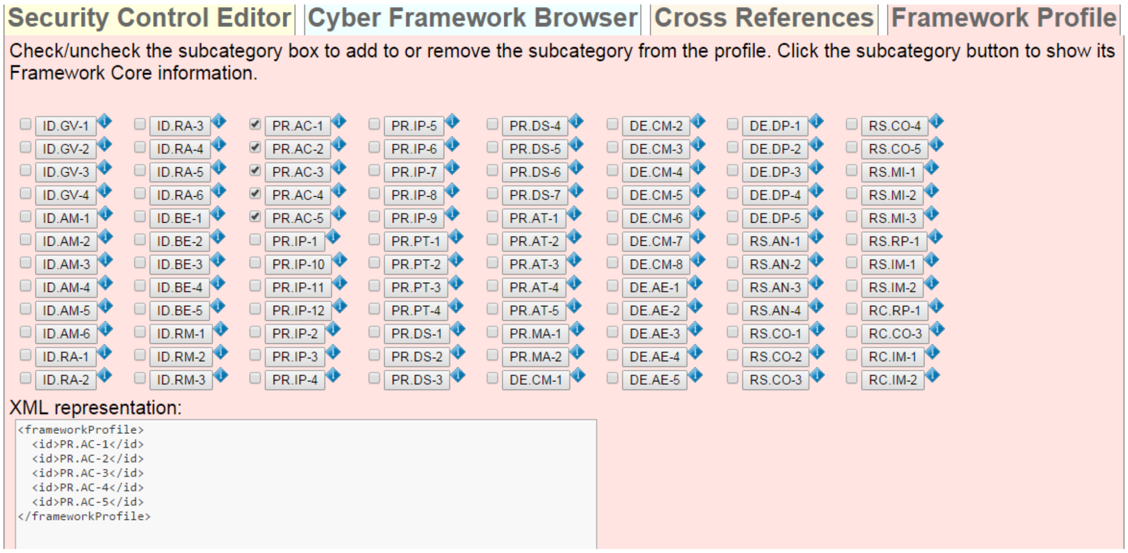
[2] Baseline Tailor's Security Control Editor tab also creates XML output on the fly. This output is generated from another dynamic model instance that encodes how the user has tailored a security control. The XML format for tailored security controls, discussed in [Lubell2015] and [Lubell2016], is both more complex and representationally richer than the simple Profile format shown in Figure 8.

Figure 7.


no
Select Profile subcategories
Select security control from informative refs
Evaluate criticality
• Cross references
• SP 800-53 def
Security control is critical?
yes
Apply additional tailoring if needed
Apply ICS overlay tailoring
yes
ICS overlay applies?
no

Workflow synthesizing Framework Core, NIST SP 800-53, and NIST SP 800-82 guidance.

Figure 8.


Security Control Editor | Cyber Framework Browser | Cross References | Framework Profile

Check/uncheck the subcategory box to add to or remove the subcategory from the profile. Click the subcategory button to show its Framework Core information.

☐ ID.GV-1
☐ ID.GV-2
☐ ID.GV-3
☐ ID.GV-4
☐ ID.AM-1
☐ ID.AM-2
☐ ID.AM-3
☐ ID.AM-4
☐ ID.AM-5
☐ ID.AM-6
☐ ID.RA-1
☐ ID.RA-2

☐ ID.RA-3
☐ ID.RA-4
☐ ID.RA-5
☐ ID.RA-6
☐ ID.BE-1
☐ ID.BE-2
☐ ID.BE-3
☐ ID.BE-4
☐ ID.BE-5
☐ ID.RM-1
☐ ID.RM-2
☐ ID.RM-3

☑ PR.AC-1
☑ PR.AC-2
☑ PR.AC-3
☑ PR.AC-4
☑ PR.AC-5
☐ PR.IP-1
☐ PR.IP-10
☐ PR.IP-11
☐ PR.IP-12
☐ PR.IP-2
☐ PR.IP-3
☐ PR.IP-4

☐ PR.IP-5
☐ PR.IP-6
☐ PR.IP-7
☐ PR.IP-8
☐ PR.IP-9
☐ PR.PT-1
☐ PR.PT-2
☐ PR.PT-3
☐ PR.PT-4
☐ PR.DS-1
☐ PR.DS-2
☐ PR.DS-3

☐ PR.DS-4
☐ PR.DS-5
☐ PR.DS-6
☐ PR.DS-7
☐ PR.AT-1
☐ PR.AT-2
☐ PR.AT-3
☐ PR.AT-4
☐ PR.AT-5
☐ PR.MA-1
☐ PR.MA-2
☐ DE.CM-1

☐ DE.CM-2
☐ DE.CM-3
☐ DE.CM-4
☐ DE.CM-5
☐ DE.CM-6
☐ DE.CM-7
☐ DE.CM-8
☐ DE.AE-1
☐ DE.AE-2
☐ DE.AE-3
☐ DE.AE-4
☐ DE.AE-5

☐ DE.DP-1
☐ DE.DP-2
☐ DE.DP-3
☐ DE.DP-4
☐ DE.DP-5
☐ RS.AN-1
☐ RS.AN-2
☐ RS.AN-3
☐ RS.AN-4
☐ RS.CO-1
☐ RS.CO-2
☐ RS.CO-3

☐ RS.CO-4
☐ RS.CO-5
☐ RS.MI-1
☐ RS.MI-2
☐ RS.MI-3
☐ RS.RP-1
☐ RS.IM-1
☐ RS.IM-2
☐ RC.RP-1
☐ RC.CO-3
☐ RC.IM-1
☐ RC.IM-2

XML representation:

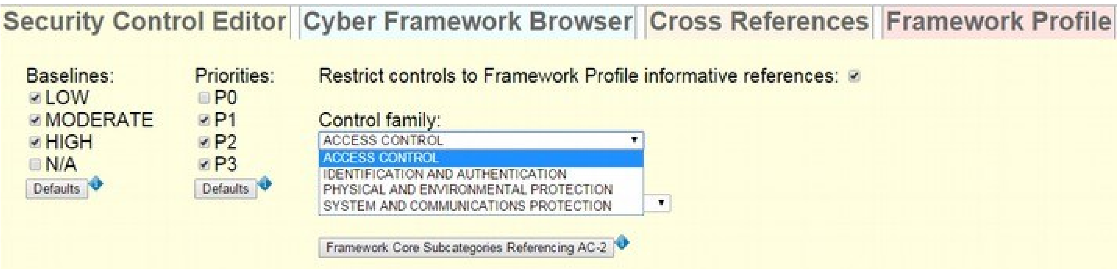
```
<frameworkProfile>
  <id>PR.AC-1</id>
  <id>PR.AC-2</id>
  <id>PR.AC-3</id>
  <id>PR.AC-4</id>
  <id>PR.AC-5</id>
</frameworkProfile>
```

Framework Profile tab.

The analyst now switches to the Security Control Editor tab and checks a box restricting control choices to only those that are referenced by subcategories of PR.AC. As shown in Figure 9, the PR.AC subcategories reference only four of the eighteen NIST SP 800-53 control families. Now suppose the analyst selects ACCESS CONTROL from the "Control family" drop-down list, and then chooses "AC-2 – ACCOUNT MANAGEMENT" from the "Control" drop-down list populated with the subset of the Access Control family that the Profile references (Figure 10). The Security Control Editor tab now displays the UI for tailoring AC-2, the upper portion of which is shown in Figure 11.[3]

[3] [Lubell2016] discusses in detail the lower portion of the tailoring UI, which has editable text fields for adding supplemental guidance and rationale, and a non-editable text field providing XML output representing the tailored control.

Figure 9.



Security Control Editor | Cyber Framework Browser | Cross References | Framework Profile

Baselines:
☑ LOW
☑ MODERATE
☑ HIGH
□ N/A
Defaults

Priorities:
□ P0
☑ P1
☑ P2
☑ P3
Defaults

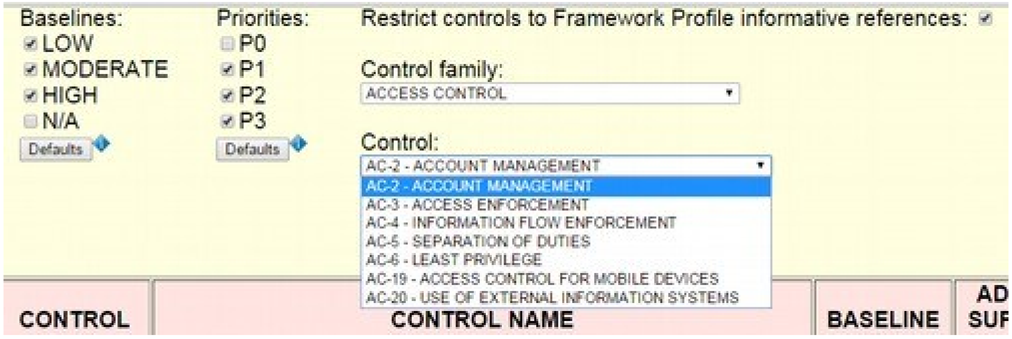
Restrict controls to Framework Profile informative references: ☑

Control family:
ACCESS CONTROL
- ACCESS CONTROL
- IDENTIFICATION AND AUTHENTICATION
- PHYSICAL AND ENVIRONMENTAL PROTECTION
- SYSTEM AND COMMUNICATIONS PROTECTION

Framework Core Subcategories Referencing AC-2

Control families referenced by PR.AC subcategories.

Figure 10.



Baselines:
☑ LOW
☑ MODERATE
☑ HIGH
□ N/A
Defaults

Priorities:
□ P0
☑ P1
☑ P2
☑ P3
Defaults

Restrict controls to Framework Profile informative references: ☑

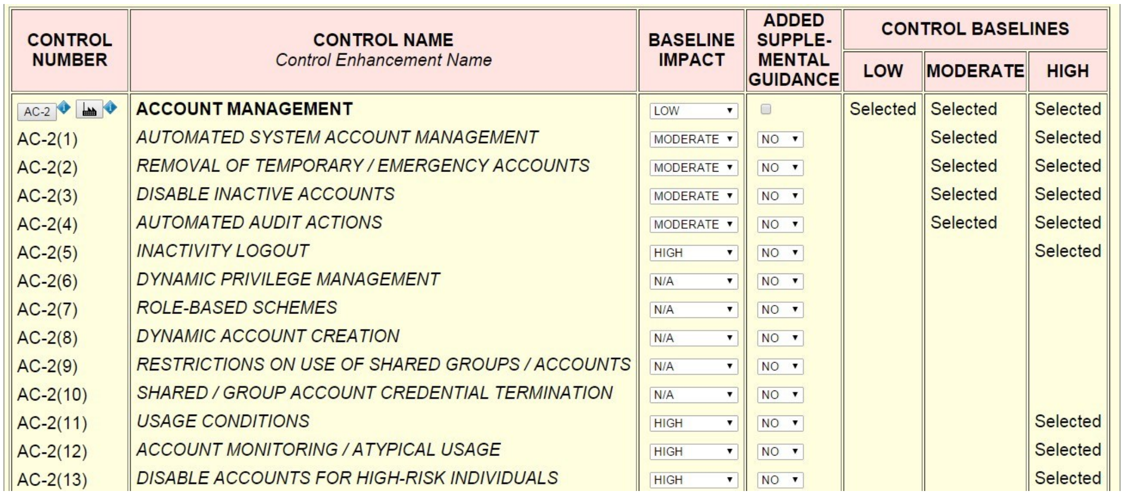
Control family:
ACCESS CONTROL

Control:
AC-2 - ACCOUNT MANAGEMENT
- AC-2 - ACCOUNT MANAGEMENT
- AC-3 - ACCESS ENFORCEMENT
- AC-4 - INFORMATION FLOW ENFORCEMENT
- AC-5 - SEPARATION OF DUTIES
- AC-6 - LEAST PRIVILEGE
- AC-19 - ACCESS CONTROL FOR MOBILE DEVICES
- AC-20 - USE OF EXTERNAL INFORMATION SYSTEMS

CONTROL | CONTROL NAME | BASELINE | AD SUF

Controls belonging to Access Control family that are referenced by PR.AC subcategories.

Figure 11.



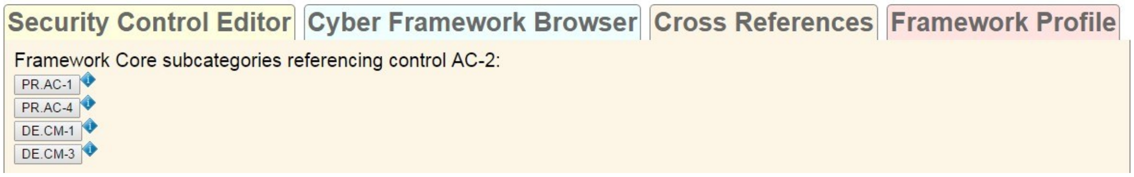
CONTROL NUMBER	CONTROL NAME *Control Enhancement Name*	BASELINE IMPACT	ADDED SUPPLE-MENTAL GUIDANCE	CONTROL BASELINES		
				LOW	MODERATE	HIGH
AC-2	**ACCOUNT MANAGEMENT**	LOW	□	Selected	Selected	Selected
AC-2(1)	*AUTOMATED SYSTEM ACCOUNT MANAGEMENT*	MODERATE	NO		Selected	Selected
AC-2(2)	*REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*	MODERATE	NO		Selected	Selected
AC-2(3)	*DISABLE INACTIVE ACCOUNTS*	MODERATE	NO		Selected	Selected
AC-2(4)	*AUTOMATED AUDIT ACTIONS*	MODERATE	NO		Selected	Selected
AC-2(5)	*INACTIVITY LOGOUT*	HIGH	NO			Selected
AC-2(6)	*DYNAMIC PRIVILEGE MANAGEMENT*	N/A	NO			
AC-2(7)	*ROLE-BASED SCHEMES*	N/A	NO			
AC-2(8)	*DYNAMIC ACCOUNT CREATION*	N/A	NO			
AC-2(9)	*RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS*	N/A	NO			
AC-2(10)	*SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*	N/A	NO			
AC-2(11)	*USAGE CONDITIONS*	HIGH	NO			Selected
AC-2(12)	*ACCOUNT MONITORING / ATYPICAL USAGE*	HIGH	NO			Selected
AC-2(13)	*DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*	HIGH	NO			Selected

Security control AC-2.

At this point, the analyst wishes to determine security control AC-2's criticality with respect to Framework Core category PR.AC. Clicking the "Framework Core Subcategories Referencing AC-2" button in Figure 9 switches to the Cross References tab, revealing that two of the five PR.AC subcategories – PR.AC-1 and PR.AC-4 – reference AC-2 (shown in Figure 12). Concluding that security control AC-2 should be selected for implementation, the analyst clicks the AC-2 button shown in the upper left of

Figure 11 to look up AC-2's definition in the NIST SP 800-53 online database. Items *d*, *i*, and *k* in the AC-2 Control Description (Figure 13) are relevant to category PR.AC. The analyst therefore decides to go ahead and tailor AC-2 for the ICS.

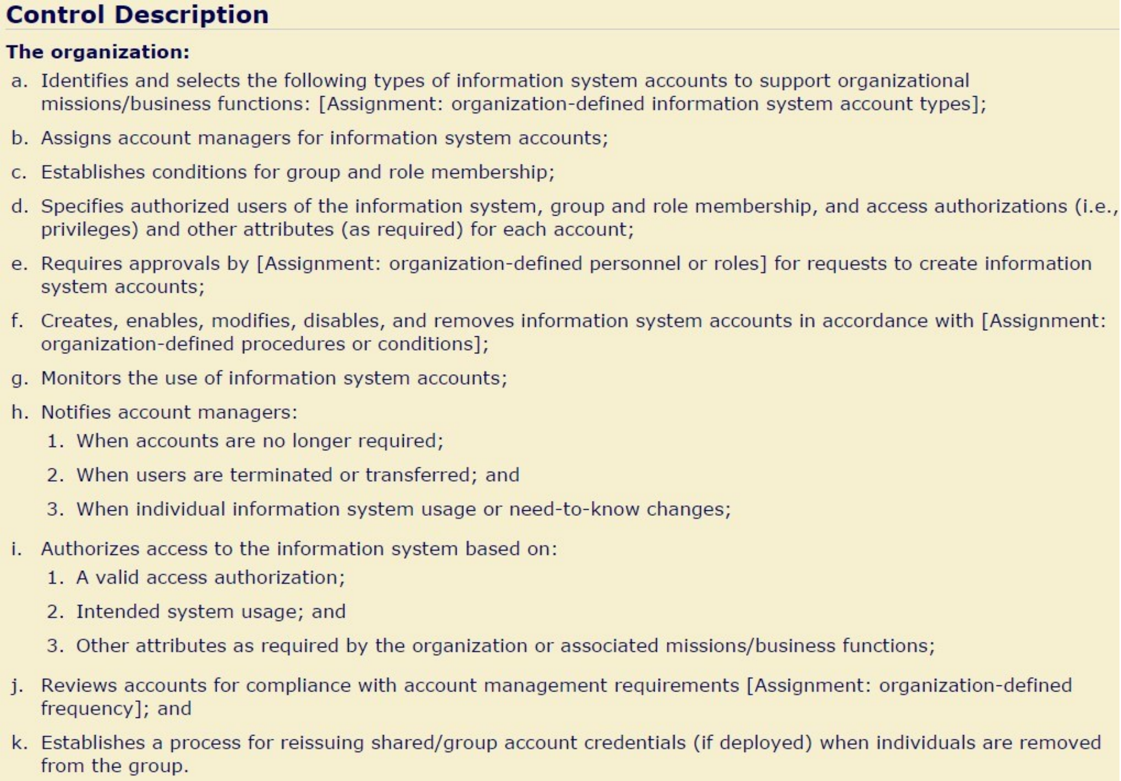
Figure 12.



Framework Core subcategories referencing control AC-2:

Subcategories referencing AC-2.

Figure 13.



Control Description

The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

g. Monitors the use of information system accounts;

h. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;

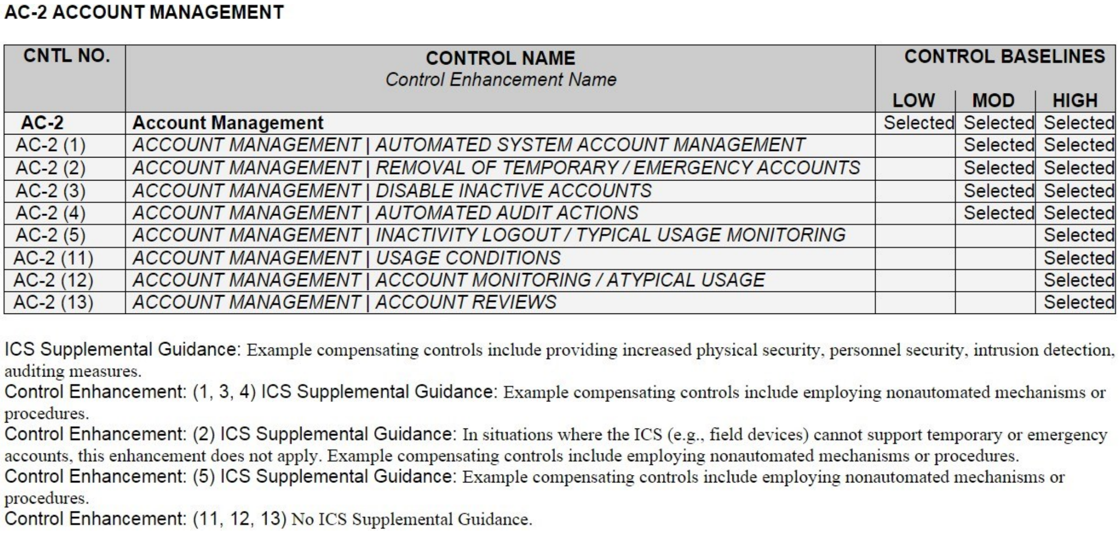
j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

NIST SP 800-53 online database: AC-2 description.

The analyst now clicks on the button with the factory image in Figure 11, to the right of the AC-2 button, to view AC-2's tailoring guidance in the NIST SP 800-82 ICS overlay. The overlay guidance (Figure 14) retains the same baseline allocation as NIST SP 800-53, but adds ICS-specific supplemental guidance suggesting compensating controls. Compensating controls are alternatives, for when the NIST SP 800-53 recommendations are not feasible, that provide comparable protection. The compensating controls mentioned in Figure 14 meet requirements specific to ICS. For example, an ICS may have limited network connectivity and only a small number of potential users, making physical security measures possibly more cost-effective than account management (where information processing overhead might impact performance). Using the NIST SP 800-82 guidance as a starting point, the analyst proceeds to tailor AC-2 using Baseline Tailor's Security Control Editor tab.

Figure 14.



AC-2 ACCOUNT MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-2	**Account Management**	Selected	Selected	Selected
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*		Selected	Selected
AC-2 (2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*		Selected	Selected
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*		Selected	Selected
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*		Selected	Selected
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT / TYPICAL USAGE MONITORING*			Selected
AC-2 (11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*			Selected
AC-2 (12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*			Selected
AC-2 (13)	*ACCOUNT MANAGEMENT | ACCOUNT REVIEWS*			Selected

ICS Supplemental Guidance: Example compensating controls include providing increased physical security, personnel security, intrusion detection, auditing measures.
Control Enhancement: (1, 3, 4) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.
Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS (e.g., field devices) cannot support temporary or emergency accounts, this enhancement does not apply. Example compensating controls include employing nonautomated mechanisms or procedures.
Control Enhancement: (5) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.
Control Enhancement: (11, 12, 13) No ICS Supplemental Guidance.

NIST SP 800-82 ICS Overlay definition: AC-2.

To summarize, the scenario discussed in this section shows how a UI implemented solely with XML technologies can increase the utility of the Framework Core, NIST SP 800-53 database, and NIST SP 800-82 ICS overlay. Baseline Tailor not only provides a common UI bringing them all together, but also derives important inter-relationships. As the example showed, a Framework Profile can be used to limit the Security Control Editor tab’s “Control family” and “Control” drop-down choices to the subset of NIST SP 800-53 security controls likely to be most relevant to the Profile. In addition, the Cross References tab can be used as a metric for a security control’s importance with respect to the Framework Core.

6. Related Research

Previous research efforts in the areas of risk management, quality and comprehension of spreadsheet data, and the use of XPath for data integration influenced the approach described in this paper.

Linkov et al. [Linkov] studied existing risk-based guidance in the nuclear power regulation, nanotechnology, and cybersecurity fields. Defining risk as the product *threat×vulnerability×consequence*, they found that in all three cases a traditional bottom-up approach was insufficient for quantifying these three variables. Reasons why included uncertainty regarding emerging threats, lack of clear guidance for risk mitigation and determining risk tolerance, and a poor understanding of stakeholders' socio-political concerns. Linkov et al. concluded that a hybrid approach combining top-down decision making with bottom-up risk analysis can make it easier for organizations to determine and manage risk. With respect to cybersecurity, Linkov et. al observed that NIST's “Guide for Conducting Risk Assessments” [SP800-30] recommends taking an organization's risk tolerance into account when assessing risk. The Framework Profile part of the Cybersecurity Framework helps in fulfilling this recommendation by providing a means for ensuring that an organization's cybersecurity strategy, risk tolerance, and mission/business objectives are all aligned.

Numerous research efforts focused on issues with spreadsheets as a means of representing and disseminating information, a common thread being the inability of spreadsheets to capture context. Context includes information such as why content was created and how it relates to other content [OAIS]. Durusau and Hunting [Durusau], citing news reports of business calamities that were caused by errors in spreadsheet data, enumerated root causes of the errors and suggested that topic maps could help in providing the missing context information. Kohlhase et al. [Kohlhase] conducted experiments that confirmed lack of context information as a major cause of semantic misunderstandings of data in spreadsheets. Hung et al. [Hung] developed a spreadsheet-like formula language to map spreadsheet data to a target schema and implemented the language as an Excel plug-in. Cunha et al. [Cunha2009a],[Cunha2009b], employing methods for automatically detecting functional dependencies, developed and implemented formalized approaches for improving spreadsheet quality.

Recent advances in cloud computing and web technologies have motivated researchers to investigate XPath and XPath-based languages as a means for integration of information from distributed sources. Pedersen et al. [Pedersen] used XPath as part of a formal semantic foundation for on-the-fly multidimensional data integration. The formalism uses XPath combined with a subset of the Structured Query Language (SQL) [Date]. Rennau and Grün [Rennau] determined that XQuery [XQuery] is a highly useful integration language for heterogeneous information sources, with the caveat that enhancements to XQuery and related standards are needed to improve navigational abilities for some non-XML sources.

7. Concluding Remarks

This paper presented a technical approach employing XSLT and XForms for developing a UI that integrates information from multiple sources. The original information sources may or may not be XML, and the original presentation may be either top-down or bottom-up. The Baseline Tailor software application validates the technical approach, adding value for cybersecurity professionals wishing to use the Cybersecurity Framework and NIST SP 800-53 guidance together. The `core.xml` static XForms model instance that provides the information displayed in the Cyber Framework Browser tab (Figure 3) a useful contribution in its own right since the current edition of the Cybersecurity Framework lacks a structured XML representation of the Framework Core. The Baseline Tailor software application, `core.xml`, and related XML resources are available at http://www.nist.gov/el/msid/baselinetailor.cfm.

Interestingly, Baseline Tailor was originally conceived as software only for tailoring the SP 800-53 security controls. A later version added the ability to browse the Cybersecurity Framework Core, but did not support bidirectional traversal of links between subcategories and security controls. Full integration came later, after the author began working with a team developing a Framework Profile for manufacturing systems. To incorporate guidance from the NIST SP 800-53 security control catalog and NIST SP 800-82 ICS overlay into the Manufacturing Profile, the team frequently needed to trace backwards from security controls to subcategories. This was cumbersome using the tables in the Cybersecurity Framework and NIST SP 800-53 documents. Baseline Tailor's Cross References tab made the task much easier. The team's experience before versus after the Cross References tab was added to Baseline Tailor validates the hybrid approach to risk management advocated in [Linkov].

A major limitation of the technical approach described in Section 3 is its reliance on hand-editing for semi-automated conversion of spreadsheet data to XML. It might be feasible to implement a more automated solution using the mapping language developed by Hung et al., or functional dependency detection methods from Cunha et al. A challenge with either automation approach would be getting spreadsheet authors to cooperate. A big attraction of spreadsheets as a medium for disseminating information is that authoring them is easy. Requiring authors to encode transformation logic as formulas or to think about functional dependencies makes spreadsheet production harder, although it may make life easier for spreadsheet consumers.

Acknowledgments

The author would like to thank KC Morris, Bob Lipman, Rick Candell, and the Balisage peer reviewers for their helpful comments on earlier drafts of this paper. Any remaining mistakes are the author's sole responsibility. Thanks are also due to the author's colleagues on NIST's Cybersecurity for Smart Manufacturing Systems project for their support and for many enlightening discussions.

Disclaimer

Mention of third-party or commercial products or services in this paper does not imply approval or endorsement by the National Institute of Standards and Technology, nor does it imply that such products or services are necessarily the best available for the purpose.

References

[CSF] National Institute of Standards and Technology (NIST) and United States of America. "Framework for Improving Critical Infrastructure Cybersecurity." (2014). http://www.nist.gov/cyberframework.

[CSFTool] "NIST Cybersecurity Framework (CSF) Reference Tool." http://www.nist.gov/cyberframework/csf_reference_tool.cfm. Accessed April 29, 2016.

[Cunha2009a] Cunha, Jacome, Joao Saraiva, and Joost Visser. "Discovery-Based Edit Assistance for Spreadsheets." In Symposium on Visual Languages and Human-Centric Computing (VL/HCC). 233–37. IEEE (2009).

[Cunha2009b] Cunha, Jacome, Joao Saraiva, and Joost Visser. "From Spreadsheets to Relational Databases and Back." In Proceedings of the 2009 ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation, 179–88. Savannah, GA, USA (2009).

[Date] Date, Chris J., and Hugh Darwen. *A guide to the SQL Standard: a user's guide to the standard relational language SQL.* Vol. 55822. Addison-Wesley Longman (1993).

[Durusau] Durusau, Patrick, and Sam Hunting. "Spreadsheets - 90+ million End User Programmers with No Comment Tracking or Version Control." Presented at Balisage: The Markup Conference 2015, Washington, DC, August 11 - 14, 2015. In Proceedings of Balisage: The Markup Conference 2015. Balisage Series on Markup Technologies, vol. 15 (2015). 10.4242/BalisageVol15.Durusau01.

[Hung] Hung, Vu, Boualem Benatallah, and Regis Saint-Paul. "Spreadsheet-Based Complex Data Transformation." In Proceedings of the 20th ACM International Conference on Information and Knowledge Management, 1749–54 (2011).

[ISO29500] ISO/IEC 29500-1:2012. "Information technology - Document description and processing languages - Office Open XML File Formats - Part 1: Fundamentals and Markup Language Reference."

[Kohlhase] Kohlhase, Andrea, Michael Kohlhase, and Ana Guseva. "Context in Spreadsheet Comprehension." Proceedings of the Second Workshop on Software Engineering Methods in Spreadsheets. Vol. 1355. Florence, Italy: CEUR Workshop Proceedings, 21-27 (2015).

[Linkov] Linkov, Igor, Elke Anklam, Zachary A. Collier, Daniel DiMase, and Ortwin Renn. "Risk-based standards: integrating top–down and bottom–up approaches." *Environment Systems and Decisions.* 34, 134–137 (2014). 10.1007/s10669-014-9488-3.

[Lubell2014] Lubell, Joshua. "XForms User Interfaces for Small Arcane Nontrivial Datasets." Presented at Balisage: The Markup Conference 2014, Washington, DC, August 5 - 8, 2014. In *Proceedings of Balisage: The Markup Conference 2014.* Balisage Series on Markup Technologies, vol. 13 (2014). 10.4242/BalisageVol13.Lubell01.

[Lubell2015] Lubell, Joshua. "Extending the Cybersecurity Digital Thread with XForms." Presented at Balisage: The Markup Conference 2015, Washington, DC, August 11 - 14, 2015. In *Proceedings of Balisage: The Markup Conference 2015.* Balisage Series on Markup Technologies, vol. 15 (2015). 10.4242/BalisageVol15.Lubell01.

[Lubell2016] Lubell, Joshua. "Baseline Tailor User Guide." NISTIR 8130. National Institute of Standards and Technology (2016). 10.6028/NIST.IR.8130.

[NVD] “NVD - 800-53.” https://web.nvd.nist.gov/view/800-53/home. Accessed April 29, 2016.

[OAIS] “Reference Model for an Open Archival Information System (OAIS).” Recommended Practice CCSDS 650.0-M-2. Consultative Committee for Space Data Systems (2012).

[Pedersen] Pedersen, Torben Bach, Dennis Pedersen, and Karsten Riis. “On-demand multidimensional data integration: toward a semantic foundation for cloud intelligence.” *The Journal of Supercomputing.* 65, 217–257 (2013). 10.1007/s11227-011-0712-3.

[Rennau] Rennau, Hans-Jürgen, and Christian Grün. “XQuery as a data integration language.” Presented at Balisage: The Markup Conference 2015, Washington, DC, August 11 - 14, 2015. In *Proceedings of Balisage: The Markup Conference 2015*. Balisage Series on Markup Technologies, vol. 15 (2015). 10.4242/BalisageVol15.Rennau01.

[SP800-30] Joint Task Force Transformation Initiative. “Guide for Conducting Risk Assessments.” NIST Special Publication 800-30. Revision 1 (2012). 10.6028/NIST.SP.800-30r1.

[SP800-53] Joint Task Force Transformation Initiative. “Security and Privacy Controls for Federal Information Systems and Organizations.” NIST Special Publication 800-53. Revision 4 (2013). 10.6028/ NIST.SP.800-53r4.

[SP800-82] Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. *Guide to Industrial Control Systems (ICS) Security.* NIST Special Publication 800-82. Revision 2 (2015). 10.6028/NIST.SP.800-82r2.

[XForms] “XForms 1.1.” W3C Recommendation (2009). http://www.w3.org/TR/xforms.

[XML] “Extensible Markup Language (XML) 1.0 (Fifth Edition).” W3C Recommendation (2008). http://www.w3.org/TR/xml.

[XPath] “XML Path Language (XPath) 3.0.” W3C Recommendation (2014). http://www.w3.org/TR/xpath-30.

[XQuery] “XQuery 3.0: An XML Query Language.” W3C Recommendation (2014). http://www.w3.org/TR/xquery-30.

[XSLT] “XSL Transformations (XSLT) Version 2.0.” W3C Recommendation (2007). http://www.w3.org/TR/xslt20.

System Interdependency Modeling in the Design of Prognostic and Health Management Systems in Smart Manufacturing

M.L. Malinowski[1], P.A. Beling[2], Y.Y. Haimes[3], A. LaViers[4], J.A. Marvel[5], and B.A. Weiss[6]

[1,2,3,4] *University of Virginia, Charlottesville, Virginia, 22904, USA*

mlm7yp@virginia.edu
beling@virginia.edu
haimes@virginia.edu
alaviers@virginia.edu

[5,6] *National Institute of Standards and Technology, Gaithersburg, Maryland, 20899, USA*

jeremy.marvel@nist.gov
brian.weiss@nist.gov

ABSTRACT

The fields of risk analysis and prognostics and health management (PHM) have developed in a largely independent fashion. However, both fields share a common core goal. They aspire to manage future adverse consequences associated with prospective dysfunctions of the systems under consideration due to internal or external forces. This paper describes how two prominent risk analysis theories and methodologies – Hierarchical Holographic Modeling (HHM) and Risk Filtering, Ranking, and Management (RFRM) – can be adapted to support the design of PHM systems in the context of smart manufacturing processes. Specifically, the proposed methodologies will be used to identify targets – components, subsystems, or systems – that would most benefit from a PHM system in regards to achieving the following objectives: minimizing cost, minimizing production/maintenance time, maximizing system remaining usable life (RUL), maximizing product quality, and maximizing product output.

HHM is a comprehensive modeling theory and methodology that is grounded on the premise that no system can be modeled effectively from a single perspective. It can also be used as an inductive method for scenario structuring to identify emergent forced changes (EFCs) in a system. EFCs connote trends in external or internal sources of risk to a system that may adversely affect specific states of the system. An important aspect of proactive risk management includes bolstering the resilience of the system for specific EFCs by appropriately controlling the states. Risk scenarios for specific EFCs can be the basis for the design of prognostic and diagnostic systems that provide real-time predictions and recognition of scenario changes. The HHM methodology includes visual modeling techniques that can enhance stakeholders' understanding of shared states, resources, objectives and constraints among the interdependent and interconnected subsystems of smart manufacturing systems. In risk analysis, HHM is often paired with Risk Filtering, Ranking, and Management (RFRM). The RFRM process provides the users, (e.g., technology developers, original equipment manufacturers (OEMs), technology integrators, manufacturers), with the most critical risks to the objectives, which can be used to identify the most critical components and subsystems that would most benefit from a PHM system.

A case study is presented in which HHM and RFRM are adapted for PHM in the context of an active manufacturing facility located in the United States. The methodologies help to identify the critical risks to the manufacturing process, and the major components and subsystems that would most benefit from a developed PHM system.

1. INTRODUCTION

Smart Manufacturing Systems require advanced technologies that facilitate widespread information flow within the system's components and subsystems. This information can include the health, performance, and risk of the system in failing to meet an objective (Jung, Morris, Lyons, Leong, & Cho, 2015). The engineering focus of Prognostics and Health Management (PHM) is coupled with smart manufacturing. The term "prognostics" refers to the prediction of the future status, health, or performance of components and systems. A commonly used metric within

Michael Malinowski et al. This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 United States License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Malinowski, M; Beling, Peter; LaViers, Amy; Marvel, Jeremy; Weiss, Brian.
"System Interdependency Modeling in the Design of Prognostic and Health Management
Systems in Smart Manufacturing." Paper presented at the Annual Conference
of the Prognostics and Health Management Society, San Diego, CA, Oct 19-Oct 24, 2015.

engineering prognostics is the remaining usable life (RUL) of a machine or system (National Institute of Standards and Technology, 2014). The term "health management" on the other hand refers to the process of making maintenance and logistics decisions from the prognostics information, available resources, and operational demand (Barajas & Srinivasa, 2008). The focus of health management is to minimize operational loss and to maximize the objectives established by the facility (Lee, Wu, Zhao, Ghaffari, Liao, & Siegel, 2014).

The use of PHM models to improve manufacturing performance has been demonstrated in numerous case studies within automotive (Holland, Barajas, Salman, & Zhang, 2010), aerospace (Batzel & Swanson, 2009), machine tool (Biehl, Staufenbiel, Recknagel, Denkena, & Bertram, 2012), and power generation (Hofmeister, Wagoner, & Goodman, 2013) industries. However, as manufacturing processes increase in size and complexity, it can become exceedingly difficult to determine which components or subsystems can most benefit from a PHM system model. Even data-driven approaches, which rely on historical data and mathematical models, lose accuracy and become less predictive as complexity increases (Bai, Wang, & Hu, 2015).

When available resources for PHM efforts are limited, designers and implementers of PHM systems face a difficult problem in deciding where to deploy these scarce resources to maximize benefit. A smart manufacturing system may involve multiple subsystems or processes that present reasonable targets for the development of PHM systems (Barajas & Srinivasa, 2008). This selection problem is made more difficult because the potential costs and benefits of those potential PHM systems are subject to random and known uncertainty (Feldman, Jazouli, & Sandborn, 2009) (Hou-bo, & Jian-min, 2011).

Numerous systems-based risk analysis methodologies designed to support decision-makers within manufacturing industries have successfully been developed and deployed (Lee, Lv, & Hong, 2013) (Fernández, & Pérez, 2015), including Hierarchical Holographic Modeling (HHM) (Haimes, 2009) and Risk Filtering, Ranking, and Management (RFRM) (Haimes, Kaplan, & Lambert, 2002) (Haimes, 2009). The original purpose of these methods (within the field of risk analysis) was to identify the most critical sources of risks to a system and to provide risk assessment, risk management, and risk communication (Haimes, 2012). With a few modifications, the critical risks identified in the HHM and RFRM processes can be used to identify the most critical components and subsystems that would most benefit from a PHM system or model.

The contribution of this paper is to introduce HHM and RFRM as methodologies to provide scope and direction for the PHM system designer. The proposed methodologies will be used to identify targets – components, subsystems, or systems – that would most benefit from a PHM system in regards to achieving the following objectives: minimizing cost, minimizing production/maintenance time, maximizing system remaining usable life (RUL), maximizing product quality, and maximizing product output. There currently exist multiple methods to determine the major failure modes of a system after an accident or catastrophe (Cocheteux, Voisin, Levrat, & Iung, 2009) (Lee et al., 2014) (Vykydal, Plura, Halfarová, & Klaput, 2015). The proposed methodology allows for a thorough analysis to be conducted even before a failure occurs in a manufacturing environment.

The remainder of the paper is organized as follows. Section 2 summarizes and explores the general HHM methodology. Section 3 explains the additional benefit of applying RFRM to the models developed using HHM. Section 4 discusses PHM-specific modifications to the RFRM method. Section 5 provides a specific case study of the application of HHM and RFRM to a major manufacturing facility. Section 6 concludes the paper.

2. HIERARCHICAL HOLOGRAPHIC MODELING, RISK ANALYSIS, AND PHM

Risk is a combined measure of the probability and severity of adverse effects (Andretta, 2014), which necessitates knowledge and understanding of future probable adverse events and their likely consequences (Haimes, 2009). To answer the basic question in risk analysis: "what can go wrong?" it is imperative that all conceivable and likely risk scenarios be identified. This is a daunting task, but can be accomplished by integrating knowledge and experience from multiple experts across different disciplines. The HHM methodology facilitates this collaboration between experts.

HHM has been successfully utilized in numerous projects and for multiple agencies, including the President's Commission on Critical Infrastructure Protection (PCCIP), the Federal Bureau of Investigation (FBI), the National Aeronautics and Space Administration (NASA), the Virginia Department of Transportation (VDOT), and the U.S. Army National Ground Intelligence Center (NGIC) (Haimes, 2009) (Lambert, Haimes, Li, Schooff, & Tulsiani, 2001). The PCCIP utilized HHM to determine the major hardware, software, human, and environmental risks to a supervisory control and data acquisition system (Chittester, & Haimes, 2004). The FBI developed an HHM model to identify varying perspectives, motives, and weaknesses between homeland defenders and terrorist networks (Haimes, & Horowitz, 2004). For VDOT, the HHM method identified major interdependencies within Virginia's transportation infrastructure and outlined critical sectors that were most sensitive to disruptions (Crowther, Dicdican, Leung, Lian, & Williams, 2004). Finally for the Army NGIC, HHM was used prior to a major deployment to identify the critical state variables of the target host country, U.S. forces, and U.S. allies (Dombroski, Haimes, Lambert, Schlussel, & Sulcoski, 2002).

Haimes (2009) defines HHM as a holistic philosophy and methodology aimed at capturing and representing the essence of the inherent diverse characteristics and attributes of a system. These system attributes include, but are not limited to, the multiple aspects, perspectives, facets, views, dimensions, and hierarchies. The mathematical and systems approach to holographic modeling reveals the interconnectedness, and the interdependencies among the system's objective functions, constraints, decision variables, and inputs/outputs (Haimes, 2009). The term holographic refers to the desire to have a multi-view image of a system (Crowther et al., 2004). For example, the risk to a system due to emergent forced changes (EFCs) can be represented from its multiple perspectives, which are related to time and geography, and include, but are not limited to: (1) economic, (2) health, (3) technical, (4) political, and (5) social perspectives. To capture a holographic outcome, the modeling team that performs the analysis must represent a broad array of experience and knowledge (Haimes, 2009).

The HHM process considers risks at both the macroscopic (management) and microscopic (component) levels. Most organizational and technology-based manufacturing systems are hierarchical in nature (Alvandi, Bienert, Li, & Kara, 2015) (He, Zhang, & Li, 2014), and the deployments of HHM have effectively addressed the risks at these multiple levels (Haimes, Kaplan, & Lambert, 2002). HHM is especially useful in determining the reliability and maintainability of infrastructures that feature a large number of components and subsystems. From a mathematical standpoint, *reliability* refers to the probability that a system is operational in a given time period, while *maintainability* is defined as the probability that a failed system can be restored to an operational state within a specified period of time (Haimes, 2009). Both of these metrics are essential to holistic risk assessment and management.

The HHM methodology produces a multilevel decomposition of a system into its many subsystems and components. This breakdown is essential to revealing the complexity and internal hierarchical nature of large-scale systems (He et al., 2014). Decomposition also allows for trade-off analyses and studies to be performed at the component, subsystem, or total system level. Applying the HHM methodology requires an organized team of experts with varied experience and knowledge bases to develop a holographic view of a system with its multiple levels and hierarchies. Although it is possible for individual experts to create different decompositions, the aggregate will yield the same optimal solution. Each expert will provide their own perspective to enforce the desired multi-view image of the system and reveal unique vulnerabilities (Kaplan, Haimes, & Garrick, 2001). Two major types of risks and uncertainties will ultimately come to light: those resulting from 1) exogenous events such as new legislation or natural disasters, and 2) endogenous events such as hardware, software, organizational, and human failures (Haimes, 2009). While knowledge of both types of events is crucial to understanding the entire system, a PHM system will focus more heavily on potential endogenous events which can take the form of critical EFCs.

At their cores, both PHM and risk analysis share two common goals: (1) to ensure that the systems under consideration perform their intended functions and meet their objectives at acceptable tradeoffs and within an acceptable time frame, and (2) to inform decision-makers so they can better predict and respond to faults and failures (Haimes, 2009) (NIST, 2015). Additionally, both practices utilize systemic risk modeling, assessment, management, and communication to achieve their goals (Ahmad & Kamaruddin, 2012) (Al-Habaibeh & Gindy, 2000). Due to these commonalities, the risk analysis theory and methodology of HHM was utilized in a case study to determine the conceivable sources of risk to a system, and finally to help decide where to apply a PHM model within a smart manufacturing facility.

3. RISK FILTERING, RANKING, AND MANAGEMENT

In total risk management, it is necessary to identify, prioritize, assess, and manage potential risk scenarios to a large-scale system. Stakeholders and decision-makers must consider the likelihoods and consequences of each risk to produce acceptable mitigation options. The Risk Filtering, Ranking, and Management (RFRM) methodology offers eight major phases to guide total risk management in an HHM system (Haimes, 2002). The eight phases are: 1 – Scenario Identification, 2 – Scenario Filtering, 3 – Bi-criteria filtering, 4 – Multi-criteria Evaluation, 5 – Quantitative Ranking, 6 – Risk Management, 7 – Safeguarding Against Missing Critical Items, and 8 – Operational Feedback. Details on these eight phases can be found in (Haimes, 2002).

The guiding force behind RFRM is the identification of head topics, which represent major concepts or perspectives of success, and subtopics, which provide detailed requirements or sources of risk (Haimes, 2009). However, it is often impractical to evaluate hundreds of sources of risk when evaluating a large system. Therefore, the risk scenarios and sources should be filtered based on professional experience, expert knowledge, and statistical data. It is also important to consider a variety of risks such as those related to hardware, software, organizational failure, human error, budget, schedule slip, and performance criteria (Haimes, 2002).

The RFRM methodology has been successfully deployed on numerous systems for multiple agencies, including the NASA, the Federal Aviation Administration (FAA), the VDOT, the National Ground Intelligence Center (NGIC), and the Department of Homeland Security (DHS) (Haimes, 2009). NASA used RFRM to identify the most common risk scenarios facing future space missions (e.g., inadequate oversight teams), and to compare management strategies to mitigate those risks (e.g., restructure existing teams or hire external consultants) (Haimes, 2009). For VDOT, the RFRM method ranked and prioritized the potential shutdowns of various transportation infrastructure assets (e.g., roads, highways, or bridges) according to their impacts on state transportation inoperability and economic loss (Crowther et al., 2004). Finally, the Army NGIC used the RFRM method to identify the risk scenarios that allied forces might encounter in a foreign country that occurred with the highest likelihood probability and produced the most severe results (e.g., loss of life or major asset) (Dombroski et al., 2002).

The risk assessment portion of RFRM can be summed up by four major questions (Haimes, 2002):

1) What can go wrong?
2) What is the likelihood of that happening?
3) What are the consequences?
4) What is the time frame?

The risk management portion on the other hand encompasses three complementary questions (Haimes, 2009):

1) What can be done and what are the available options?
2) What are the associated trade-offs in terms of costs, benefits, and risks?
3) What are the impacts of current decisions on future options?

After all relevant and potential risks have been identified as either head topics or subtopics they must be evaluated by three major criteria: resilience, robustness, and redundancy. *Resilience* refers to the ability of a system to recover after an emergency, and can be evaluated by time and resources needed. *Robustness* is the insensitivity of system performance to external stresses, so the ability to resist potential risks. *Redundancy* refers to the ability of extra components or subsystems to take over the functions of failed components or subsystems (Haimes, 2009).

The three categories of resilience, robustness, and redundancy are then further broken down into eleven essential criteria for evaluating risk scenarios (refer to Figure 1).

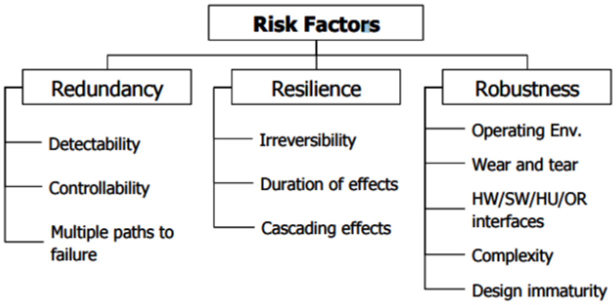


Figure 1. Risk factors with eleven criteria.

The eleven criteria relating the ability of a risk scenario to defeat the defenses of a system are formally defined as follows (Haimes, 2009):

1. *Undetectability* – the absence of modes by which the initial events of a scenario can be discovered before harm occurs
2. *Uncontrollability* – the absence of control modes that make it possible to take action or make an adjustment to prevent harm
3. *Multiple paths to failure* – multiple and possibly unknown ways for the events of a scenario to harm the system
4. *Irreversibility* – a scenario in which the adverse condition cannot be returned to the initial, operational (pre-event) condition
5. *Duration of effects* – a scenario that would have a long duration of adverse consequences
6. *Cascading effects* – a scenario where the effects of an adverse condition propagate to other systems or subsystems (cannot be contained)
7. *Operating environment* – a scenario that results from external stressors
8. *Wear and tear* – a scenario that results from use, leading to degraded performance
9. *Hardware, software, human, and organizational interfaces* – a scenario in which the adverse outcome is magnified by interfaces among one or more these subsystems
10. *Complexity/emergent behaviors* – a scenario in which there is a potential for system-level behaviors that are not anticipated even with knowledge of components and their interactions
11. *Design immaturity* – a scenario in which the adverse consequences are related to the newness of the system design or other lack of a proven concept

Each identified risk scenario must be rated as “high”, “medium”, “low”, or “not applicable” against each criterion.

Scenarios with more "high" ratings must be considered further in the RFRM process. Risk scenarios that score mostly "low" or "not applicable" in the eleven categories can be filtered out unless an emergent change drives it towards a higher level of risk. Alternative rating scales and filtering criteria could also be used with the same goal: reduction of the number of scenarios under consideration.

4. PHM-SPECIFIC MODIFICATIONS TO RISK FILTERING, RANKING, AND MANAGEMENT

The RFRM process is essential because it limits the number of risk scenarios for a manufacturing facility to a manageable quantity. However, the process must be modified to identify the risks that are applicable to realistic and practical PHM strategies. Risks that cannot be handled through PHM should still be considered at a higher system level, but will not be useful to the process described in this paper. The modifications to the standard RFRM filtering process are as follows:

M1. Risks that are rated "high" for *undetectability* should be filtered out during RFRM, unless there exists the potential to add a detection method (such as a sensor to a robot).

M2. Risks that are rated "high" for *uncontrollability* should be filtered out during RFRM, unless there exists potential to insert control modes to the process or subsystem.

M3. Risks that are directly related to only the *operating environment* and thus cannot be mitigated on a day-to-day basis should be filtered out during the RFRM.

M4. Risks that can be directly classified as either "human" or "organizational" should be filtered out during RFRM.

M5. Risks that are only rated "high" in the category of design immaturity should be filtered out during RFRM.

The purpose of the M1 modification is to ensure that only risks that can be detected, identified, and diagnosed will remain after the filtering process. This is because PHM systems rely on prognostics, and thus require predictive capabilities of future health, performance, or RUL of subsystems. They must have a means to detect or sense in order to provide effective health management. However, it should be noted that if it is possible to add a detection method or even a reliability model to the risk in question, then it should not be filtered out on the basis of the M1 modification.

The M2 modification seeks to eliminate risks that have no existing control channels. The purpose of a PHM system is to modify decision variables or inputs to a system in order to create a desired outcome. However, even if the optimal modifications to the variables can be identified, if there is no way to implement them, then there is no benefit to the system. It was additionally noted that if it is possible to add control modes, then this filtering criterion can be ignored.

The purpose of the M3 modification is to filter out risks that are *only* related to the operating environment. Specifically, these are the risks pertaining to external factors over which there is no control, such as the weather, plant location, and even legislation or industry standards. These risks should be filtered because they cannot be managed on a day-to-day basis and would require solutions outside the scope of a manufacturing PHM system. It should be noted that this should only serve as a filter if it is the only "high" rated risk category.

Modification M4 removes any risks that are primarily classified as either "human" or "organizational." The purpose here is to eliminate risks that are primarily related to issues that are difficult to control, such as human error or the organizational structure of a corporation. While managing these risks may prove extremely beneficial to a manufacturing facility, there is little opportunity for a PHM system.

Finally, the M5 modification removes risks that are focused on immature or experimental subsystems, which are usually still undergoing optimization or usability testing. These new systems will naturally inherit additional risk since they have not yet been verified. Therefore, we would not want to allocate resources towards developing a PHM system for a new component until it has become stable within its own design cycle.

5. CASE STUDY IN THE APPLICATION OF HHM AND RFRM TO PHM IN SMART MANUFACTURING

The process for identifying the most important sources of risk involves developing a Hierarchical Holographic Model and performing a PHM-oriented Risk Filtering, Ranking, and Management. As a proof of concept for this methodology, consider the following example featuring the packaging process at a major manufacturer located in the United States. Due to the competitive nature of the industry, specific details about the company have been omitted. For the remainder of this paper, the manufacturing facility shall be referred to as Plant A.

5.1. Plant A Packing and Bagging Overview

One of the major processes at Plant A encompasses the packing, transporting, and bagging of their finished product. Refer to Figure 2 for a detailed system diagram of the entire process with the major components, subsystems, sensors, machines, robots, and humans identified.

Once the product has been processed and fully prepared, it is stored on the floor in a sterilized section of the plant. A small end-loader pushes controlled heaps of the product into a grate in the floor that is outfitted with an automated screw conveyor. This screw moves the product up to a storage tank overhead, which then funnels the product to one of a few bagging stations: two 15.88 kg – 22.68 kg bag stations and one jumbo station for bulk product. After the product enters the funnels, an automated machine fills bags to their correct, preset weight. Bags are administered by human workers, one at each station. The human operators take empty bags, load them onto the filler, and then start the filling process. Finally they remove the full bags and shift the bags over to a conveyor where they are sealed, flattened, and sent down the line.

At this point the bags are in queue for a robotic palletizer. The palletizer receives sealed and inspected bags of product and stacks them onto wooden pallets in regular, repeating patterns that can be selected and adjusted by the operator. A forklift is used to remove the finished pallet where it is wrapped in shrink wrap and placed in a holding area for distribution. A central programmable logic controller with a touch screen interface coordinates the overall unit automation that was supplemented by at least six human workers: one end-loader driver, two baggers, one inspector, and two to shrink wrap finished pallets and insert empty pallets to the palletizer cage. The insertion of empty pallets into the robot workspace is accomplished by a light curtain that would turn off when the pallet was completely loaded (and the robot switched to an empty pallet on its other side) so that the loaded pallet could be removed (via forklift) and a new wooden pallet re-inserted (by a human operator who would return the light curtain to active to let the robot know it could switch back to that side when it finished the pallet on its other side).

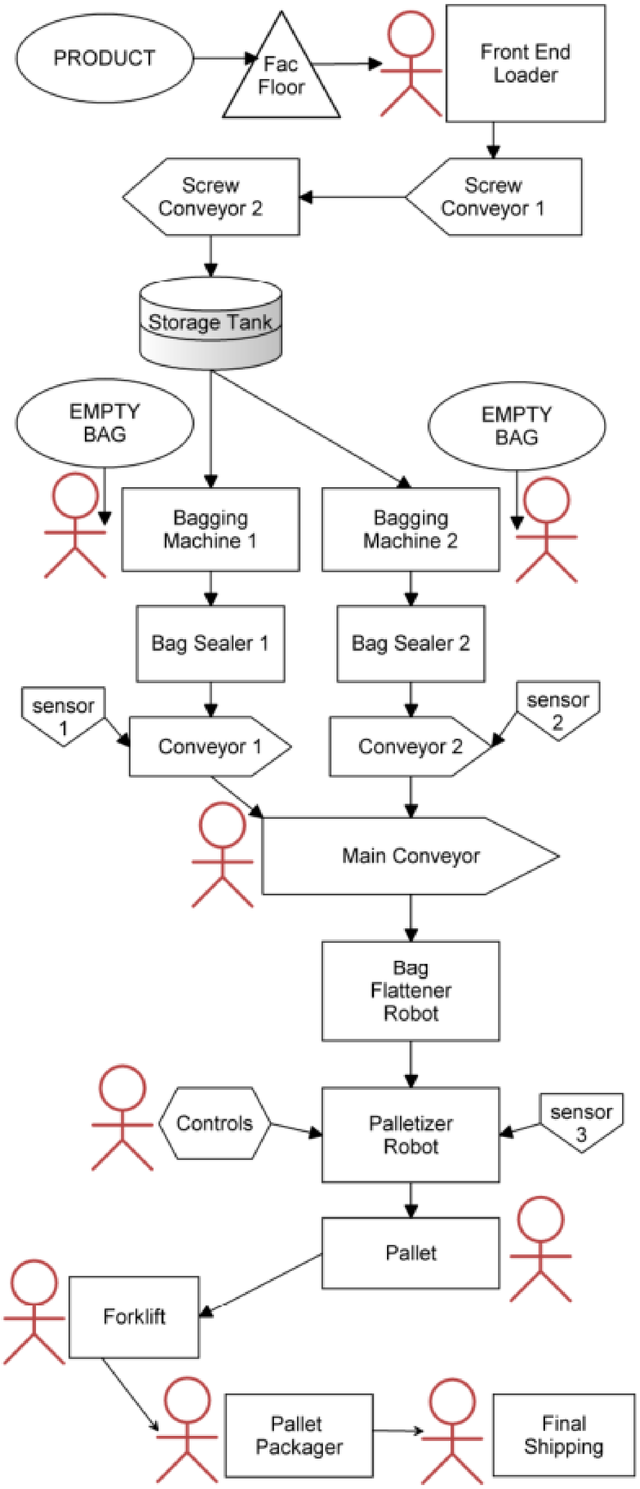


Figure 2. System diagram of Plant A.

Plant engineers have noted the following known health management issues:

- The funnel openings can become clogged with finished product if not regularly cleaned out.
- Sensors fail with regularity. Common causes of failure include occlusion of optical components by dirt and misalignment through collision with bags of product.
- The maneuvering of heavy bags by human workers is a potential source of slower productivity for the facility.
- Adjusting and reprogramming the palletizer is difficult and generally outside the scope of the work done in house. The robot engineer must be on call and able to reprogram the machine in-person.

5.2. Application of HHM and RFRM

The main objectives of the manufacturer are to maximize production of their packaged product, and to minimize the risk of a system failure (production shutdown or delay). To help achieve these objectives, Plant A wishes to implement a PHM system into their packing and bagging process. However, they currently have limited monetary resources allocated towards this effort. Thus, Plant A requires a full analysis regarding which of their components/machines/subsystems would most benefit from a PHM system. This necessitates a complete understanding of their current industrial process.

5.2.1. HHM for Plant A

First, multiple Hierarchical Holographic Models (HHMs) are developed covering multiple aspects of the manufacturing plant. The HHM models receive input from many different subject matter experts, stakeholders, and decision makers. For Plant A, an HHM model was originally developed with the perspective of the different *physical components* within the finished product bagging system. The head topics for the model were (1) Machines and Robots, (2) Components, (3) Humans, and (4) Environment. Underneath these major topics, subtopics and possible risk scenarios can be identified. The HHM model for the *physical components* has been displayed in bullet form below.

1. Machines and Robots
    a. Front End Loader
    b. Screw Conveyor
        i. Horizontal
        ii. Vertical
    c. Storage Tank Dispenser
    d. Bagging Machine
        i. Bag grip
        ii. Locking mechanism
        iii. Sensor
        iv. Product dispenser
    e. Bag Sealer
        i. Heat sealer
        ii. Conveyor belt
    f. Automated Conveyor
        i. Sensor
        ii. Belt
    g. Bag Flattener
    h. Palletizer
        i. Sensor
        ii. Arm
        iii. Claw
        iv. Controls
    i. Forklift
    j. Pallet Packager
2. Components
    a. Finished Product
    b. Bags
    c. Pallets
    d. Packaging material
3. Humans
    a. Front end loader driver
    b. Baggers
    c. Inspectors
    d. Forklift driver
    e. Packager
4. Environment
    a. Factory Floor
    b. Storage Tank
    c. Air
    d. Moisture
    e. Contaminants

A similar HHM model was also developed from multiple experts covering a new perspective: the different *processes* within the finished product bagging system. The practice of creating multiple HHM models helps to provide a holographic view of the entire system and ensure that the major sources of risk are properly captured. It provides a more realistic and complete overall model by recognizing the limitations of modeling a complex system with just a single structure. The head topics for the *processes* model were (1) Storing Product, (2) Transporting Product, (3) Bagging Product, (4) Sealing Bags, (5) Transporting Bags,

(6) Flattening Bags, (7) Stacking Bags on a Pallet, and (8) Preparing Final Product for Delivery. The complete HHM model can be seen in bullet form below.

1. Storing Product
    a. Environment
        i. Factory floor
        ii. Air
        iii. Moisture
    b. Human interactions
    c. Factory contaminant controls
2. Transporting Product
    a. Front end loader
        i. Scoop product
        ii. Push product into floor grates
    b. Screw conveyors
        i. Move product to vertical conveyor
        ii. Move product to storage tank
3. Bagging Product
    a. Human operator
        i. Obtain empty bag
        ii. Fill bag
    b. Bagging machine
        i. Grip bag
        ii. Lock bag
        iii. Sense weight
        iv. Unlock bag
    c. Storage tank
        i. Open hatch to drop product
        ii. Close hatch to secure product
4. Sealing Bags
    a. Human operator
        i. Place bag
    b. Bag sealer
        i. Sense bag
        ii. Grip bag
        iii. Heat seal bag
        iv. Transport bag
        v. Lay bag flat
5. Transporting Bags
    a. Human supervisor
        i. Controls
        ii. Fix unaligned bags
    b. Automated conveyor
        i. Sense bags
        ii. Move bags
        iii. Delay bags
6. Flattening Bags
    a. Human supervisor
        i. Controls
    b. Bag flattener
        i. Sense bag
        ii. Flatten bag
        iii. Move bag
7. Stacking Bags on a Pallet
    a. Forklift
        i. Move empty pallet to palletizer
    b. Human supervisor
        i. Adjust settings for palletizer
        ii. Start/stop process
        iii. Fix fallen bags
    c. Palletizer robot
        i. Sense bag
        ii. Grip bag
        iii. Lift bag
        iv. Position bag
        v. Drop/place bag on pallet
8. Preparing Final Product for Delivery
    a. Forklift
        i. Lift pallet with stacked bags
        ii. Transport to packager
    b. Pallet packager
        i. Rotate pallet
        ii. Dispense shrink wrap
    c. Human operator
        i. Operate machinery
        ii. Transport completed pallet to storage area

Multiple HHM perspectives can be explored to further improve the overall system model, such as organizational, technological, or even social. For this particular case study, the *processes* perspective was used to develop risk scenarios for the finished product packing and bagging system.

5.2.2. RFRM for Plant A

Next the Risk Filtering, Ranking, & Management (RFRM) method was applied to the HHM model containing the *processes* within the product packing and bagging system. Each head topic was re-defined as a risk scenario, where the process in question failed to occur. Head topics 2 through 8 were identified as being the most critical to the success of the manufacturing system. The subtopics directly related to the operating environment or human interactions were then filtered out, as per the PHM-specific RFRM modifications. The remaining risk scenarios of interest are identified in Table 1 below.

Table 1. Risk scenarios of interest for RFRM

Risk ID	Risk Description
2.b	Screw conveyor failure
3.b	Bagging machine failure
3.c	Storage tank failure
4.b	Bag sealer failure
5.b	Automated conveyor failure
6.b	Bag flattener failure
7.c	Palletizer robot failure
8.b	Pallet packager failure

Next a qualitative severity-scale matrix was applied to the remaining subtopics to filter out the topics that did not meet a predetermined risk threshold. A combination of expert insight from the manufacturers and historic data provided both the evidence for the evaluation and the severity of the impact levels. The results of the matrix are displayed in Table 2 below. The five likelihood/probability columns refer to the probability that an event would normally occur. For example, events in the first column occur with a probability of less than 1%, while events in the second column occur with a probability between 1% and 5%. The descriptions for the matrix scales are displayed in Table 3 and Table 4 below.

Table 2. Severity-scale matrix for identified risk scenarios.

Impact	Likelihood/Probability				
	Pr<0.01	Pr<0.05	Pr<0.1	Pr<0.5	Pr<1
4		7.c			
3	3.c	2.b	3.b		
2		5.b, 8.b		6.b	
1	4.b				
0					

Table 3. Risk description for severity matrix

Low Risk	Moderate Risk	High Risk	Extremely High Risk

Table 4. Impact description for severity-scale matrix

Impact #	Impact Description
4	Entire Production Shutdown
3	Loss of Product
2	Reduced Production Speed
1	Minor Equipment Degradation
0	Minor or No Effect

According to the RFRM methodology, the topics classified as either "High Risk" or "Extremely High Risk" must be further evaluated, while the other scenarios can be filtered out. In this case, the remaining risk scenarios were:

3.b – Bagging machine failure

6.b – Bag flattener failure

7.c – Palletizer robot failure

These scenarios must be analyzed for their ability to defeat the major defensive properties of a system: redundancy, resilience, and robustness. This can be determined by rating their performance along the eleven criteria RFRM attributes of risk scenarios, displayed in Table 5.

Table 5. Eleven RFRM attributes of risk scenarios.

#	Criteria
1	Undetectability
2	Uncontrollability
3	Multiple paths to failure
4	Irreversibility
5	Duration of effects
6	Cascading effects
7	Operating environment
8	Wear and tear
9	Hardware/software/human/organizational
10	Complexity and emergent behaviors
11	Design immaturity

Each category receives a qualitative assessment regarding whether the risk scenario has a low, medium, or high susceptibility to the given criterion. The evaluation for the three remaining risk scenarios within the Plant A example can be seen below (refer to Table 6).

Table 6. Assessment of risk scenarios using eleven criteria.

Criteria #	3.b Bagging	6.b Flatten	7.c Palletize
1	Medium	Medium	High
2	Low	Low	Low
3	Medium	Low	High
4	Medium	Low	Medium
5	Low	Medium	Medium
6	Medium	Medium	High
7	Medium	Low	Medium
8	Medium	Medium	Medium
9	High (human)	Low	High
10	Low	Low	Medium
11	Low	Low	Low

Finally, the PHM-specific RFRM modifications must be checked against the three identified risk scenarios. It can be seen that the palletizer robot failure (7.c) rated high for *undetectability* (1), so according to the PHM modifications it should be removed. However in this case we opt to keep this risk scenario since there are sensors available which can be added to the palletizer robot as detection methods. Additionally the bagging machine failure (3.b) received a high rating for *hardware/software/human/organizational* (9), but only because it was classified as a strictly "human" process. For this reason this risk scenario can be filtered out before further analysis.

5.2.3. Results and Findings from HHM and RFRM

After eliminating risks using the PHM-specific RFRM rules, the palletizer robot received the highest risk assessment both in the qualitative severity-scale matrix (refer to Table 2) and within the eleven attributes of risk (refer to Table 6). Therefore, the HHM and RFRM methodologies have successfully identified an essential location within the Plant A bagging and packaging process. We are confident that the application of a PHM effort at the palletizer robot will provide the biggest impact towards achieving the main objectives: maximizing production and minimizing the risk of a system failure (production shutdown or delay).

Given limited resources, it is recommended that the product manufacturer begin by implementing a PHM strategy at the palletizer robot, and then if available resources remain, proceed with the other top identified sources of risk. The components of the palletizer (arms, claws, sensors, controls, etc.) can even be evaluated for their individual levels of risk to determine which ones are most critical to the palletizer subsystem. Then a variety of PHM methodologies can be implemented for the palletizer to develop an optimal risk management solution for the entire smart manufacturing system-of-systems. This analysis may be crucial in the development of low-level process management by creating awareness of the interconnected system of systems that manufacturing plants rely on to operate efficiently, safely, and in a timely manner. This holistic understanding should trickle down to inform the structure and communications of future robotic control architecture.

6. CONCLUSION

As smart manufacturing facilities increase in size and complexity, it becomes exceedingly challenging to apply Prognostics and Health Management (PHM) models and strategies to the entire system without recognizing and addressing this emergent complexity as a system of systems. This paper has described a systems-based risk-analysis methodology capable of identifying all conceivable sources of risk to smart manufacturing process in support of PHM.

The well-developed practice of risk analysis provides two powerful tools for this methodology: HHM and RFRM. The original purpose of these methods within the risk analysis field was to identify the most critical risks to a system and to provide risk assessment, risk management, and risk communication. However as demonstrated in this paper, with a few modifications the critical risks identified in the HHM and RFRM processes can provide scope and direction for the PHM system designer. Specifically, HHM and RFRM can be utilized to identify the major components, subsystems, or systems that would most benefit from a PHM system while prioritizing the following manufacturing objectives: minimizing cost, minimizing production and maintenance time, maximizing system remaining usable life (RUL), maximizing product quality, and maximizing product output.

NIST DISCLAIMER

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

ACKNOWLEDGEMENT

This paper documents results from a collaborative effort between the University of Virginia's Systems Engineering Department, and the National Institute of Standards and Technology (NIST).

REFERENCES

Ahmad, R., & Kamaruddin, S. (2012). An overview of time-based and condition-based maintenance in industrial application. *Computers & Industrial Engineering*, vol. 63 (1), pp. 135-149.

Al-Habaibeh, A., & Gindy, N. (2000). A new approach for systematic design of condition monitoring systems for milling processes. *Journal of Materials Processing Technology*, vol. 107 (1), pp. 243-251.

Alvandi, S., Bienert, G., Li, W., & Kara, S. (2015). Hierarchical modelling of complex material and energy flow in manufacturing systems. *Procedia CIRP*, vol. 29, pp. 92-97.

Andretta, M. (2014). Some considerations on the definition of risk based on concepts of systems theory and probability. *Risk Analysis*, vol. 34 (7), pp. 1184-1195.

Bai, G., Wang, P., & Hu, C. (2015). A self-cognizant dynamic system approach for prognostics and health management. *Journal of Power Sources*, vol. 278, pp. 163-174. doi:10.1016/j.jpowsour.2014.12.050.

Barajas, L. G., & Srinivasa, N. (2008). Real-time diagnostics, prognostics and health management for large-scale manufacturing maintenance systems. *ASME 2008 International Manufacturing Science and Engineering Conference collocated with the 3rd JSME/ASME International Conference on Materials and Processing* (pp. 85-94). American Society of Mechanical Engineers.

Batzel, T. D., & Swanson, D. C. (2009). Prognostic health management of aircraft power generators. In *IEEE Transactions on Aerospace and Electronic Systems*, vol. 45 (2), pp. 473-482.

Biehl, S., Staufenbiel, S., Recknagel, S., Denkena, B., & Bertram, O. (2012). Thin film sensors for condition monitoring in ball screw drives. *1st Joint International Symposium on System-Integrated Intelligence: New Challenges for Product and Production Engineering*.

Chittester, C. G., & Haimes, Y. Y. (2004). Risks of terrorism to information technology and to critical interdependent infrastructures. *Journal of Homeland Security and Emergency Management*, vol. 1 (4).

Cocheteux, P., Voisin, A., Levrat, E., Iung, B. (2009). Prognostic design: requirements and tools. *11th International Conference on The Modern Information Technology in the Innovation Processes of the Industrial Enterprises*, MITIP 2009. Bergame, Italy.

Crowther, K. G., Dicdican, R. Y., Leung, M. F. , Lian, C., & Williams, G. M. (2004). Assessing and managing risk of terrorism to Virginia's interdependent transportation systems. *Center for Risk Management of Engineering Systems*, Charlottesville, Virginia.

Dombroski, M., Haimes, Y. Y., Lambert, J. H., Schlussel, K., & Sulcoski, M. (2002). Risk-based methodology for support of operations other than war. *Military Operations Research*, vol. 7 (1), pp. 19-38.

Feldman, K., Jazouli, T., & Sandborn, P. (2009). A methodology for determining the return on investment associated with prognostics and health management. *IEEE Transactions on Reliability*, vol. 58 (2), pp. 305-316.

Fernández, F. B., & Pérez, M. Á. S. (2015). Analysis and modeling of new and emerging occupational risks in the context of advanced manufacturing processes. *Procedia Engineering*, vol. 100, pp. 1150-1159.

Haimes, Y. Y. (3rd ed.). (2009). *Risk modeling, assessment, and management*. Hoboken, NJ: John Wiley & Sons, Inc.

Haimes, Y. Y. (2012). Systems-based guiding principles for risk modeling, planning, assessment, management, and communication. *Risk Analysis*, vol. 32 (9), pp. 1451-1467.

Haimes, Y. Y., & Horowitz, B. M. (2004). Adaptive two-player hierarchical holographic modeling game for counterterrorism intelligence analysis. *Journal of Homeland Security and Emergency Management*, vol. 1 (3).

Haimes, Y. Y., Kaplan, S., & Lambert, J. H. (2002). Risk filtering, ranking, and management framework using hierarchical holographic modeling. *Risk Analysis*, vol. 22 (2), pp. 383-397. doi:10.1111/0272-4332.00020.

He, N., Zhang, D. Z., & Li, Q. (2014). Agent-based hierarchical production planning and scheduling in make-to-order manufacturing system. *International Journal of Production Economics*, vol. 149, pp. 117-130.

Hou-bo, H., & Jian-min, Z. (2011). Cost-benefit model for PHM. *Procedia Environmental Sciences*, vol. 10, pp. 759-764.

Hofmeister, J. P., Wagoner, R. S., & Goodman, D. L. (2013). Prognostic health management (PHM) of electrical systems using condition-based data for anomaly and prognostic reasoning. *Italian Association of Chemical Engineering*, vol. 33, pp. 991-996. doi: 10.3303/CET1333166.

Holland, S. W., Barajas, L. G., Salman, M., & Zhang, Y. (2010). PHM for automotive manufacturing & vehicle applications. *Prognostics & Health Management Conference Fielded Systems Session*, October 14, Portland, Oregon.

Jung K., Morris K. C., Lyons K. W., Leong S., & Cho H. (2015). Mapping strategic goals and operational performance metrics for smart manufacturing systems. *Procedia Computer Science*, vol. 44, pp. 184-193. doi:10.1016/j.procs.2015.03.051.

Kaplan, S., Haimes, Y. Y., & Garrick, B. J. (2001). Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk. *Risk Analysis*, vol. 21 (5), pp. 807-807.

Lambert, J. H., Haimes, Y. Y., Li, D., Schooff, R. M., & Tulsiani, V. (2001). Identification, ranking, and management of risks in a major system acquisition. *Reliability Engineering & System Safety*, vol. 72 (3), pp. 315-325.

Lee, C. K. M., Lv, Y., & Hong, Z. (2013). Risk modelling and assessment for distributed manufacturing system. *International Journal of Production Research*, vol. 51 (9), pp. 2652-2666.

Lee, J., Wu, F., Zhao, W., Ghaffari, M., Liao, L., & Siegel, D. (2014). Prognostics and health management design for rotary machinery systems – Reviews, methodology and applications. *Mechanical Systems and Signal Processing*, vol. 42 (1-2), pp. 314-334. doi:10.1016/j.ymssp.2013.06.004.

National Institute of Standards and Technology (NIST). (2015). Measurement science roadmap for prognostics and health management for smart manufacturing systems. *Roadmapping Workshop on Measurement Science for Prognostics and Health Management of Smart Manufacturing Systems*. November 19-20, 2014, Gaithersburg, MD.

Vykydal, D., Plura, J., Halfarová, P., & Klaput, P. (2015). Advanced approaches to failure mode and effect analysis (FMEA) applications. *Metalurgija*, vol. 54 (4), pp. 675-678.

BIOGRAPHIES

Michael L. Malinowski earned a B.S. in Aerospace Engineering from the University of Virginia (UVA), Charlottesville, VA, USA, 2012. He is currently pursuing an M.S. degree in Systems Engineering from UVA. He worked as a Systems and Test Engineer at Lockheed Martin Corporation between 2012 and 2014, and graduated from their Engineering Leadership Development Program within the Mission Systems and Training business division. He also worked as an Engineer at Science Applications International Corporation between 2009 and 2012. He is a member of AIAA, Tau Beta Pi, and Sigma Gamma Tau. His research interests are risk assessment and management of engineering systems.

Peter A. Beling received his Ph.D. in Operations Research from the University of California, Berkeley, CA, USA. He is an associate professor in the Department of Systems and Information Engineering at the University of Virginia (UVA). He is active in the UVA site of the Broadband Wireless Applications Center, which an Industry-University Cooperative Research Center sponsored by the National Science Foundation. His research interests are decision making in complex systems, with an emphasis on adaptive decision support systems and on model-based approaches to system-of-systems design and assessment. His research has found application in a variety of domains, including prognostics and health management, mission-focused cyber security, and financial decision-making.

Yacov Y. Haimes received his Ph.D. in Large-Scale Systems Engineering from the University of California, Los Angeles, CA, USA, 1970. He is the Founding Director (1987) of the Center for Risk Management of Engineering Systems at the University of Virginia. On the faculty of Case Western Reserve University, Cleveland, OH, for 17 years he was the Chair of the Systems Engineering Department, and Director of the Center for Large-Scale Systems and Policy Analysis. Between 1977 and 1978, he was an AAAS/American Geophysical Union Congressional Science Fellow, joining the staff of the Executive Office of President Jimmy Carter, and later the staff of the House Science and Technology Committee. He has published more than 250 articles and technical papers, edited or co-edited 21 volumes, and authored or co-authored 6 books.

Amy LaViers earned a B.S.E. in Mechanical and Aerospace Engineering from Princeton University, Princeton, NJ, USA. She completed an M.S. and Ph.D. in Electrical and Computer Engineering at the Georgia Institute of Technology, Atlanta, GA, USA. She is an Assistant Professor in Systems and Information Engineering and Director of the Robotics, Automation, and Dance Lab at the University of Virginia. She aims to extract useful features from human movement for robotic applications, such as endowing co-robots the ability to work alongside human workers in manufacturing plants.

Jeremy A. Marvel received his Ph.D. in Computer Engineering from Case Western Reserve University, Cleveland, OH, USA, 2010. He is a project leader and research scientist in the Intelligent Systems division of the National Institute of Standards and Technology (NIST) in Gaithersburg, MD. Since joining the research staff at NIST, he has established the Collaborative Robotics Laboratory, which is engaged in research dedicated to developing test methods and metrics for the performance and safety assessments of collaborative robotic technologies. His research focuses on intelligent and adaptive solutions for robot applications, with particular attention paid to human-robot collaborations, multi-robot coordination, safety, perception, self-guided learning, and automated parameter optimization. He is currently engaged in developing measurement science methods and artifacts for the integration and application of robots in collaborative assembly tasks for manufacturing.

Brian A. Weiss earned a B.S. in Mechanical Engineering (2000), Professional Masters in Engineering (2003), and Ph.D. in Mechanical Engineering (2012) from the University of Maryland, College Park, Maryland, USA. He is currently the Associate Program Manager of the Smart Manufacturing Operations Planning and Control program and the Project Leader of the Prognostics and Health Management for Smart Manufacturing Systems project within the Engineering Laboratory (EL) at the National Institute of Standards and Technology (NIST). He spent 15 years conducting performance assessments across numerous military and first response technologies including autonomous unmanned ground vehicles, tactical applications operating on Android devices, advanced soldier sensor technologies, and urban search and rescue robots. His efforts have earned him numerous awards including a Department of Commerce Gold Medal (2013), Silver Medal (2011), Bronze Medals (2004 & 2008), and the Jacob Rabinow Applied Research Award (2006).

ASME 2016 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference
IDETC2016
August 21-24, 2016, Charlotte, North Carolina

IDETC2016-60216

USING INDUSTRY FOCUS GROUPS AND LITERATURE REVIEW TO IDENTIFY CHALLENGES IN SUSTAINABLE ASSESSMENT THEORY AND PRACTICE

Matteo M. Smullin
School of Mechanical, Industrial, and
Manufacturing Engineering
Oregon State University
Corvallis, Oregon 97331
smullinm@oregonstate.edu

Karl R. Haapala
School of Mechanical, Industrial, and
Manufacturing Engineering
Oregon State University
Corvallis, Oregon, 97331, USA
Karl.Haapala@oregonstate.edu

Mahesh Mani
Dakota Consulting Inc.
Silver Spring, MD 20901
&
Systems Integration Division
National Institute of Standards and Technology
Gaithersburg, MD 20899

KC Morris
Systems Integration Division
National Institute of Standards and Technology
Gaithersburg, MD 20899

ABSTRACT

The bottom up demand from consumers for more sustainable products, and the top down need to comply with government regulations motivates manufacturers to adopt tools and methods to evaluate their operations for opportunities to reduce environmental impact and improve competitiveness. Manufacturers have actively improved the sustainability of their products through the use of such tools and methods. However recently, manufacturers are struggling to maintain the necessary gains in energy and material efficiency due to the assessment inaccuracies of current ad hoc methods and their inability to identify large sustainability improvement opportunities. Overcoming this barrier requires standardized methods and tools that are implementable and which contain accurate manufacturing process-level information. To aid in developing such methods and tools, this study contrasts the perspective of industry and academic research on the topics of sustainable manufacturing metrics and measurements, and process modeling to determine the deficits that exist in enacting academic theory to practice. Furthermore, this study highlights some of the industry responses to the development of related standards for sustainability assessment.

INTRODUCTION

Sustainable manufacturing is defined as the creation of manufactured products using processes that minimize negative environmental impacts, conserve energy and natural resources; are safe for employees communities and consumers; and are economically sound [1]. To that end, researchers have created methods to assess the environmental, social, and economic impacts of manufactured products or processes through a myriad of indicators and metrics [2–4].

Over the past two decades, studies have repeatedly emphasized a lack of accurate tools and methods to support sustainable manufacturing. A 2002 workshop on environmentally benign manufacturing [5] supported the consensus that better assessment tools and more accurate data are needed. Bunse et al. [6] reported on the implementation gap between academic theory and industrial practice. Through interviews they affirmed their initial hypothesis that standardized tools and methods could speed up the adoption of sustainable practices. Bhanot et al. [7] published a survey in 2015 concluding that one of the main barriers to sustainable manufacturing is the lack of standards. This was supported by Rachuri et al. in 2009 [8] in an analysis of sustainable manufacturing best practices.

The work reported herein documents existing barriers related to (1) manufacturing metrics and measurements and (2) manufacturing process modeling that can support sustainable manufacturing. Findings are based on an industry perspective (focus groups) and academic perspective (literature review). Strategies for overcoming the barriers, including standards development are presented from both perspectives.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.
Approved for public release; distribution is unlimited.

Mani, Mahesh; Haapala, Karl; Smullin, Matteo; Morris, Katherine.
"Using Industry Focus Groups and Literature Review to Identify Challenges in Sustainable Assessment Theory and Practice."
Paper presented at the ASME International Design Engineering Technical Conference, Charlotte, NC, Aug 21-Aug 24, 2016.

The paper is organized as follows. First, the *Research Approach* section presents the design of industry focus groups (here, called roundtables), as well as supporting literature on methods for conducting qualitative research. The *Literature Perspective* section is presented as two subsections reviewing the literature on (1) manufacturing metrics and measurements and (2) manufacturing process modeling. Next, the *Industry Perspective* on the two focus areas is presented, based on the roundtables. The *Research Findings* section presents barriers and gaps identified by contrasting the industry and literature perspectives. Further, this section tabulates the identified barriers and recommended changes to foster standards development and adoption. Next, the *Relevant Standards Efforts* section presents current standards and their capabilities. Finally, the *Conclusions* section presents underlying trends identified from the research, as well as directions of future work.

RESEARCH APPROACH

To investigate the two focus topics of this research, i.e., metrics and measurement, and process modeling, from the perspective of the literature and industry, a literature review was conducted and three roundtables were hosted to gather a relevant body of key findings (Fig. 1). These findings were then compared to identify barriers and gaps and to support the introduction of academic theory to industry practice.

The literature review was organized and conducted as a traditional literature review. This type of review identified and summarized the literature on one or more chosen topics. The primary focus was to develop a comprehensive background illuminating current research findings [9,10]. The literature review investigated three subtopics due to their influence on the two overarching focus topics. Thus, to summarize the literature perspective of manufacturing metrics, measurements, and manufacturing process modeling required investigating root causes. The literature perspectives/findings were later compared to the findings of the industry roundtable group discussions.

The industry perspective was gathered by hosting three roundtables meetings from June 2015 to March 2016. The roundtables were distributed geographically to gather a diverse set of industry participants and information since companies tend to cluster to achieve greater competitiveness [11]. A small group of 8-12 representatives attended each roundtable. Represented companies spanned a range of industries and sizes, from small high tech startups to well established, large manufacturing companies.

Each roundtable meeting was organized into three dialogue sessions lasting about two hours each. Each dialogue session was conducted as a focus group, however, the term “roundtable” is used hereafter to imply that the research was more academic in purpose and not to be affiliated with the more political or commercial connotations of a typical “focus group.” Questions were designed to foster discussion in each area of interest, while also allowing time for note takers to document relevant information.The intent of the first dialogue session of each roundtable was to foster discussion about performance indicators, processes, process flow and plant/facility performance, and the communication of metrics.

The intent of the second dialogue was to foster discussion about capturing and describing sustainability information at the process level to support system level decision making. Topics included manufacturing process modeling and benefits of process characterization. The third dialogue centered on measurement science as a means to characterize manufacturing processes and to systematically capture and describe sustainability information to enable better decision making.

To determine how the dialogue sessions would be conducted, the authors investigated four well-known methods for soliciting opinions from subject matter experts (Fig. 2). The four methods included the Delphi, brainstorming, nominal group technique, and focus group techniques. References [12] and [13] were reviewed by the authors to gain a sense of the respective strengths and weaknesses of each group discussion method. From the investigated methods, the authors selected the focus group method for its strength in extracting the range and diversity of participants agreements and disagreements [14]. Focus groups are a research technique to collect data based on personal experience and opinion from a set of participants presented with a question from a researcher. Krueger and Casey [14] established some of the first guidelines for applying the focus group technique. The guidelines recommend that a focus group be conducted in three phases: conceptualization, interview, and analysis.

In the conceptualization phase, questions are designed to elicit specifics, but remain open ended. Following this guideline, a set of five key questions were formulated and discussed by the research team to ensure they remained specific, and logically sequenced.

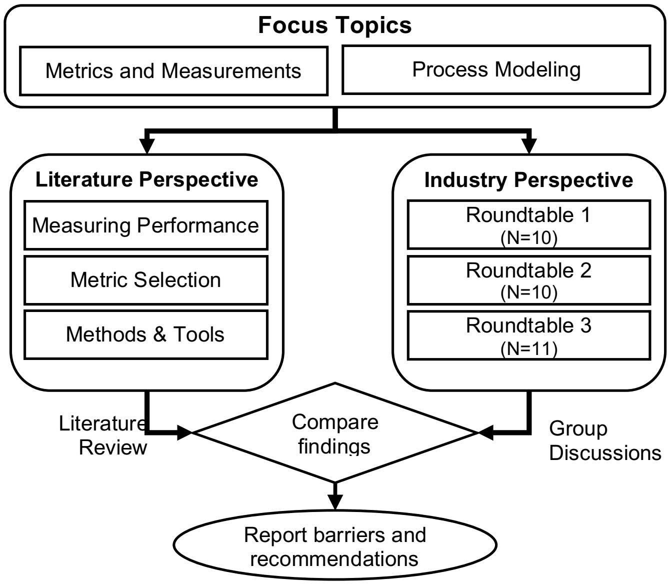


FIGURE 1: METHODOLOGY FOR IDENTIFYING DEFICITS IN THEORY AND PRACTICE FOR EACH FOCUS AREA

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.
Approved for public release; distribution is unlimited.

Mani, Mahesh; Haapala, Karl; Smullin, Matteo; Morris, Katherine. SP-619
“Using Industry Focus Groups and Literature Review to Identify Challenges in Sustainable Assessment Theory and Practice.”
Paper presented at the ASME International Design Engineering Technical Conference, Charlotte, NC, Aug 21-Aug 24, 2016.

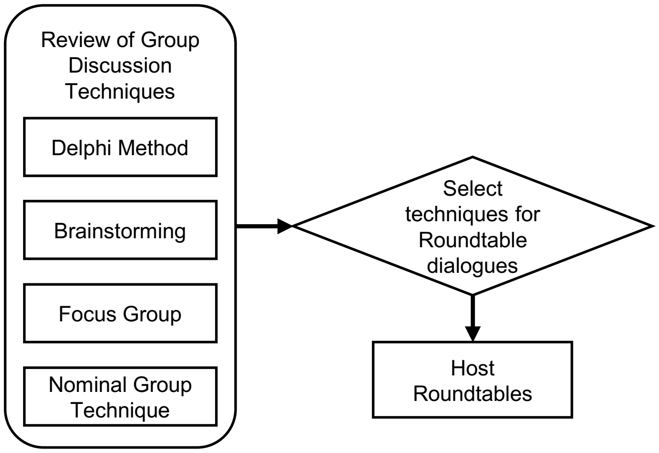

Review of Group Discussion Techniques
Delphi Method
Brainstorming
Focus Group
Nominal Group Technique
Select techniques for Roundtable dialogues
Host Roundtables

FIGURE 2: DESIGN OF THE ROUNDTABLE DIALOGUES

In the interview phase, the moderator, who is knowledgeable on the discussion topics, begins the discussion with a welcome, overview, and ground rules before asking the first question [14]. Time is allocated to allow participants to socialize prior to the discussion. In keeping with this guideline the authors designed the roundtables to allow informal greetings over a continental breakfast before formally welcoming and introducing the participants to the dialogue topics. Furthermore, focus groups are designed such that each participant individually responds to the moderator's question with their own opinions. To ensure this, the roundtable moderator walked within the perimeter of the open circle of participants and questioned each participant in round-robin style on each topic. When each participant had voiced their answer, the floor was opened for group discussion.

The guideline for the analysis phase instructs a research team to collect and collate all notes, analyze the notes either quantitatively or qualitatively, and distribute the results to participants. Following this guideline, the notes collected by the researchers were collated and compared. Raw data was qualitatively described and interpreted and reported out to participants and the research team observers to achieve consensus on the interpreted findings. The findings are described in the Industry Perspective section, below. The key ideas from each roundtable are reported. Where available, specifics are given to substantiate the claims in the form of quotes or mentioned tools and methods.

LITERATURE PERSPECTIVE

The literature perspective is presented on the two focus topics 1) Manufacturing Metrics and Measurements, and 2) Manufacturing Process Modeling. Each focus topic was approached by assessing the relevant literature in identifying how sustainable manufacturing performance is measured, how metrics are selected, and how methods and tools are applied in practice.

Manufacturing Metrics and Measurements

Over the last twenty years, studies have detailed the necessity for sustainable manufacturing metrics and indicators, the means for determining what metrics to use, and how they should be deployed. Indicators and metrics relate sustainability performance areas to each other and to the process in question (Fig. 3).

Each performance area can have one or more indicators. In turn, an indicator can be described by one or more metrics. Indicators provide a context to measure, analyze, and score sustainability aspects of manufacturing processes. For example, the social performance area might include an indicator for occupational health and safety (OH&S) and could be assessed on the performance of the related metrics, such as number of acute injuries. Indicators can be defined internally, or selected from various indicator repositories. Evaluation metrics associate the process(es) to be evaluated with the identified indicator [15] [16]. Some of the earliest proposed sustainability indicators and metrics were sourced from life cycle assessment (LCA) [17,18], and used to evaluate company performance [19]. These indicators were categorized by Joung et al. [3] who discovered that, while there is a large number of social indicators, there are few related social metrics. In part, the lack of social metrics is due to the inability to accurately quantify a number of qualitative indicators [27].

The most common indicators include material, energy, and waste [20] as they are tactile and easily measurable. Other authors noted that only recently have efforts incorporated system level indicators into the final sustainability decision making process [21]. Only recently has focus shifted towards extending indicators and measurement methods to cover factory, system, and unit process impacts. Linke et al. [22] developed process level metrics for use in grinding operations, noting that grinding require different metrics than other processes [23]. Further, only recently have methods been devised to account for factory overhead, such as HVAC systems, into the decision making process for production [24]. However, in an interesting dichotomy, as more metrics and measurement methods have been introduced and the process flows been made more complex [25], the number and scope of tools available to aid sustainability assessment for decision makers has multiplied to unmanageable levels [26,27].

The perceived deficit in metrics for the social performance area has not interrupted the profusion of unique tools and methods for assessing sustainability. From the perspective of industry, however, these tools tend to be limited in relevancy as a result of being either too narrow in focus, and thus myopic, or too broad in focus, and therefore inaccurate [28]. Furthermore, the tools often do not consider the technical or cultural maturity of the organization and thus contain no provisions for adaptability [29]. A need has arisen for simple, easy to use tools [26] that are standardized, well-rounded, and well-communicated to individual companies [30], as well as scalable to meet the maturity of companies' sustainability endeavors.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.
Approved for public release; distribution is unlimited.

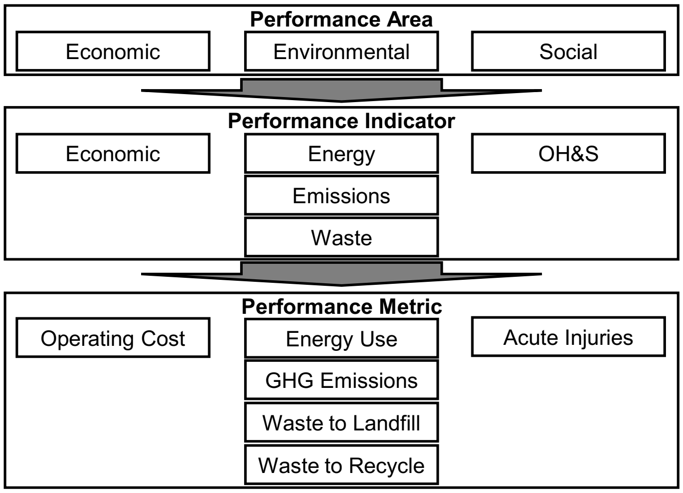


FIGURE 3: MANUFACTURING INDICATORS/METRICS [31]

In light of the findings of the literature review, the questions posed during the dialogue were designed to address these deficits and gather useful information for wider distribution to the research community.

1. What approaches do companies use to understand process-level issues and their effects on system-level performance?
2. How are manufacturing performance indicators selected?
3. What tools, methods, and systems are used to capture and track manufacturing-process level performance indicators?

Manufacturing Process Modeling

While the research into manufacturing process modeling has seen advancements (see [32,33]), the prevailing methods and tools employed by small and medium size enterprises (SMEs) to characterize and assess the sustainability performance of their processes are diverse and *ad hoc* [28]. This is the result of a deficit in standards development for modeling processes and conducting sustainable performance assessments. Standards for representing manufacturing processes and the collection of sustainability-related data would support sustainability analysis and facilitate reuse of that data in multiple types of analyses [16][15].

Central to a process model is the unit manufacturing process (UMP). UMPs have two inherent themes. The first considers that the UMP is the smallest element in manufacturing [1]. The second is that value is added through a specific shape, structure, or property transformation. UMP models are developed to explore process and material interactions, and can be used to quantify sustainability metrics [34]. The models, developed through mechanistic relationships or empirical observations [31] relate material and energy inputs to outputs and can account for variations in the process. A process model represents a process or set of processes by incorporating process and workpiece analytics. This allows reusability of the model in sustainable manufacturing evaluations. A process model links the internal transformation of inputs to outputs to the evaluation metrics selected for final performance evaluation [35] (Fig 4).

In the process model, the transformation of the workpiece requires a set of inputs, which are then converted into output form. In the figure, each input arrow is uniquely drawn to emphasize a special characteristic. Information relays the process and workpiece parameter settings, and can enable composing of UMP models. Consumables are expended through use and outputted as wastes or emissions. Energy is transformed, not consumed in the traditional sense. Labor is a necessary input that can result in labor hazards, or injuries imparted to the worker. For each set of inputs and outputs, a set of evaluation metrics connected to selected performance indicators that can be tracked to determine the system performance.

A brief review of the literature revealed what research has been conducted in the field and what deficits exist that could benefit from industry inputs. The first process models used theoretical physics to estimate the impact of the chosen environmental indicators [36]. Later process models were more empirically based, such as the energy models developed by Gutowski et al. [37] and Li and Kara [38]. More recently, the CO2PE! initiative developed models using a standard unit process life-cycle inventory approach (UPLCI) [39]. UPLCI was defined by Overcash and Twomey [40] to contain an overview of the process, literature data and references, a parameter selection of the process, life-cycle inventory (LCI) energy calculations, and LCI mass loss calculations. The intent of this method is to bridge the gap between UMP modeling and LCA and has been used to model the energy and material flows of laser sintering and stereolithography [41], and grinding [42] to more transparently and accurately determine the environmental impact of the respective processes.

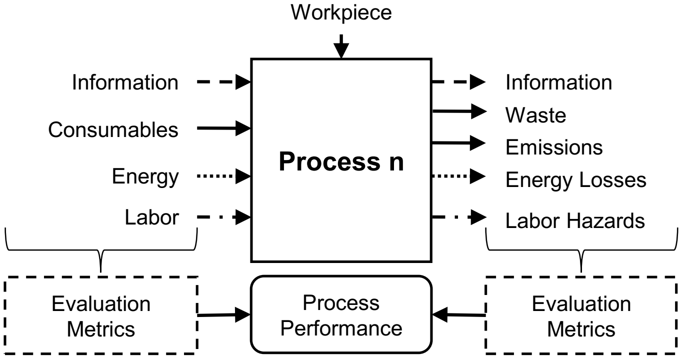


FIGURE 4: UMP MODEL SCHEMATIC WITH PLACEMENT OF SUSTAINABLE EVALUATION METRICS ADAPTED FROM GARRETSON [35]

Others have worked to aid decision making in UMP modeling through benchmarking [43], focusing only on waste, energy, and materials [20], or attending to the variability, information, and modeling uncertainty inherent in UMP models by incorporating Bayesian Networks [44]. Model uncertainty has been investigated using Monte Carlo simulation [45]. Extending the work of integrating sustainability into the supply chain, Kremer et al. [46] reasoned that supply chain methods and tools

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.
Approved for public release; distribution is unlimited.

fail in industry applications for a number of reasons, e.g., exclusion of manufacturing process modeling from "what if" analysis when selecting suppliers.

The literature review identified several deficits related to manufacturing process modeling: First, there are challenges in determining the most accurate method for modeling a given process; second, there are challenges in allocation of system overhead to the process level; and third, there is a lack of simple tools to first model unit processes and subsequently link them together. The dialogue on manufacturing process modeling was designed around these central concerns. The questions asked were:

1. What is the value of modeling manufacturing processes?
2. How does your company characterize individual manufacturing processes?

INDUSTRY PERSPECTIVE

The following section reports on the findings from the industry roundtable dialogues related to manufacturing metrics and measurements. The second section reports on the findings from the dialogues on manufacturing process modeling.

Manufacturing Metrics and Measurements

When asked what approaches their companies had used to understand the effect of process-level issues on system-level performance, participants overwhelmingly identified using metric heavy approaches including such metrics as defect rate and labor cost. The companies represented at the roundtables used a variety of methods to assess the quality of their products (e.g., defect detection systems, flow analysis, data analysis, and on-line inspection). Standards for judging quality are typically set industry wide; however, no standard exists for how to measure quality. For example, a representative from the wood products industry mentioned their company built windows in two different facilities. The final quality grade was the same, however, the measurement method used to inspect build quality differed.

On the topic of sustainability performance, the consensus was that most sustainability assessments focus only on system level environmental and social indicators and metrics and are commonly conducted in consultation with LCA practitioners. The intent of these sustainability assessments is to identify areas for improvements, though these can become quickly exhausted if the focus is only system level indicators (e.g., factory energy consumption and total waste). To identify new improvement opportunities requires tracking and reporting process-level data and information.

Means for tracking the process-level issues include various types of control and monitoring devices. Historical data is used to identify root causes of process issues and map process responses to control parameters. For example, a carbon nanotube manufacturer required 2-3 years of data to understand process operation. Another common approach identified was the use of factory floor operator experience, go/no go gauges, and, generally, holding line managers accountable for process control. Identifying and selecting metrics for process-level tracking is often done based on the experience of managers and line operators and only in response to specific problems.

The result is that metrics and their related process equations are not standard and often are not documented in a standard manner, if at all, and many metrics rely on a controller's tacit knowledge of the process. This lack of standardization and reliance on expert knowledge leads some business units to be starved of data, while others are inundated. Standards (e.g., AS 9001) were discussed by a few participants as a means of addressing the data and metric disparity by centralizing a common core of measurements, metrics, and indicators.

When asked if currently utilized indicators and metrics originated and were communicated from top down or bottom up, participants identified waste generated and safety, alongside quality, as common top-down performance metrics. Common bottom-up metrics are those that are quantifiable, e.g., energy, water, and waste – with waste appearing to be the only commonality. In general, bottom-up metrics are reactively developed to meet the mandated top-down (often regulatory) indicators. Compliance is achieved by employing bottom-up metrics to improve modeling accuracy and system performance at the process level. Industry also proactively select indicators to improve quality or to reduce the risk of environmental accidents. Some are even selecting indicators to gain sustainability minded customers or benchmarking against other companies using indices (e.g., Dow Jones Sustainability Index).

However, industry continues to struggle with the organizational difficulties of reconciling bottom up with top down indicators and metrics. The same is true for communication of information and goals among different business units. This disconnect is due to business autonomy with the result that both bottom-up and top-down data and metrics often become siloed within a business unit.

Communication between engineering departments and shop floor operations was identified by managers as a continuing struggle. Oftentimes communication is one sided, with management sending work instructions to shop floor personnel with no intention of receiving feedback. This wall between management engineering and shop floor was widely agreed upon by participants as the largest contributor to system, process, and product issues. Furthermore, there was common agreement that it can be difficult to engage shop floor personal to enact top down initiatives. A few participants noted that in their experience, incentives such as cash handouts or dashboards can act as pushes to overcome these barriers.

In summary, most metrics and measurement methods are selected on the experience of the managers. Repeated on a large scale, this compartmentalization leads to a lack of uniform and formally-defined metrics and methods to capture manufacturing process data across an industry. This lack of standardization inhibits industry's ability to benchmark and collectively learn best practices. Furthermore, without standardized metrics and measurements, standardized process models cannot be successfully created. The topic of manufacturing process modeling is presented in the next section. Manufacturing process modeling was the focus of the third and final dialogue session.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.
Approved for public release; distribution is unlimited.

Manufacturing Process Modeling

The first question asked of participants gathered high-level inputs on the perceived value of manufacturing process modeling and the use of tools for manufacturing process modeling. One of the more prominent values is the increased prediction accuracy compared to control or monitoring only. The literature review concluded that UMP modeling has the capability to increase the accuracy of sustainability assessments by quantifying resources in the form of labor and machine hours, equipment utilization, energy, and water use to produce a product or perform a process. Yet, due to the number of competing tools and methods advocated by the literature, industry is loath to adopt a new method or tool from a yet to be standardized field. For example, participants noted that other time-tested techniques (e.g., Six Sigma and lean techniques) or tools (e.g., ARENA) accomplish the desired quality and accuracy goals.

This reluctance extends to the adoption of new resources. Common resources dedicated to process modeling include software for computational fluid dynamics (CFD), input-output mass and energy balances and process flow analysis (e.g., Aspen), environmental impact (e.g., SolidWorks Sustainability), solid modeling (e.g., Pro/ENGINEER), and specialized tools in MS Excel. Process failure modes and effects analysis (P-FMEA) has been used, but does not have suitable off-the-shelf tools for sustainability analysis. In most cases these tools are not equipped to facilitate UMP modeling. Most software tools address sustainable design-for-manufacture but not the sustainability of the manufacturing processes themselves. Furthermore, these tools often lack accurate databases, forcing companies to construct unique internal databases.

From a mathematical standpoint, manufacturing process transformations are calculated using first principles. For activities requiring more accuracy, companies turn to empirical modeling. Model uncertainty is handled using Monte Carlo analysis, and some participants noted seeing Bayesian analysis used in practice. In both cases, these techniques are applied piece-wise to a single chosen process. Moving from the process to the facility, process flow diagrams and material flow analysis are sometimes used for modeling plant layout, plant replication, and plant improvement.

In summary, industry is hesitant to adopt UMP modeling for a number of reasons. First, the sustainability literature shows little cohesion or unison in advocating a common approach to UMP modeling. This makes industry wary to adopt methods and tools that run the risk of become obsolescent. Second, industry is aware that the benefits of UMP modeling may not be apparent until after the models have been developed, but the nascent state of UMP research reduces the industries willingness to invest the resources necessary to create these models. In the next section, the results of comparing the two perspectives are presented as a discussion on the perceived barriers to the adoption of standards and recommended changes to current practices.

RESEARCH FINDINGS

Based on a comparison of the literature review and the industry roundtables, a set of identified barriers and recommendations was developed. This set emerged by identifying deficits between theory and practice. They are presented below in tabular form (Table 1 and Table 2).

Comparing the findings from literature with the results of the roundtables illustrates several key findings where literature and industry diverge in theory and practice of UMP modeling. The summary conclusion from industry is that product quality remains the key process indicator. Supported by lean principles, the implicit understanding is that increasing quality at the process level reduces system level costs. Yet, the sustainable manufacturing literature on the topic of product quality as an indicator and metric is brief. Product surface quality has seen extensive research [23,47,48], however, this work is still in the minority from sustainability perspective. For example, in a recently proposed sustainable indicator framework to aid small manufacturers, only one indicator could be directly related to product quality, and the rest measure the costs related to manufacture of the product and not the product itself [49]. This also alludes to the discrepancy between sustainable metrics and accounting principles. That is, few metrics explicitly connect the sustainability performance of UMPs to cost competitiveness. Furthermore, while the literature details many bottom-up metrics, the consensus among larger, more mature industries is that top-down metrics dominate as dictated by government regulations. Recently, there has been a trend in the sustainability research field to respond by incorporating elements of public policy and governance into sustainability tools and methods [50]. The need is for bottom-up metrics that satisfy top-down compliance requirements. Industry and academia are working to address these issues, such as with the development of process metrics to aid tracking of social indicators, e.g., worker safety [35]. Even if all of the above situations were solved, industry participants adamantly noted that the final hurdle often encountered in conducting sustainable performance assessments is due to the breadth of the available specialized tools. The lack of standardization in sustainability assessment methods has led to a profusion of individual tools encapsulating different methods [51].

Proposed solutions to this and other identified barriers are presented in the following Relevant Standards Efforts section.

RELEVANT STANDARDS EFFORTS

This section presents the current standards capable of addressing the identified industry concerns. Existing manufacturing standards provide instructions for designers, engineers, builders, operators and decision makers to conduct activities within their fields. They also facilitate communication between stakeholders across different organizational borders. Furthermore, standards facilitate information transfer across borders of the manufacturing system hierarchy and between life cycle phases. Standards are fundamental to advanced manufacturing systems to facilitate the delivery of information to the right place at the right time. Standardization enables automating system responses and permits establishing repeatable processes all sharing common functional understanding. This reduces the cost of adopting new technology.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.
Approved for public release; distribution is unlimited.

Mani, Mahesh; Haapala, Karl; Smullin, Matteo; Morris, Katherine. SP-623
"Using Industry Focus Groups and Literature Review to Identify Challenges in Sustainable Assessment Theory and Practice."
Paper presented at the ASME International Design Engineering Technical Conference, Charlotte, NC, Aug 21-Aug 24, 2016.

TABLE 1: IDENTIFIED BARRIERS TO THE ADOPTION OF STANDARDIZED SUSTAINABLE ASSESSMENT TOOLS AND METHODS

Manufacturing Metrics & Measurements	
• Current tools do not emphasize usability with their steep learning curves	• Standards cannot address the needed cultural change to address sustainability in a proactive manner
• No standard method exists for combining process and system level indicators in a holistic manner	• Sustainability R&D projects do not receive equal funding within companies
• Current tools and methods do not always show immediate practical change; a necessity for adoption by industry	• Standards do not address the potential for falsification of material or process data by companies
• Recertification of a manufacturing process after modification is a financial barrier to wider standards adoption	• Sustainability metrics included in standards do not explicitly address quality; a common measure of performance amongst companies and individuals
• Companies and suppliers hesitate to share sensitive process data or models for fear of losing trade secrets or competitive advantage	• Tools and methods will not be widely adopted if they require the upgrade or replacement of analogue, but still functional, machinery
• Incorporating new methods, tools, or standards requires large time investments before showing practical results	• Current research lacks a cohesive theory on how to evaluate and close the design-for-manufacturing gap
Manufacturing Process Modeling	
• Regulatory changes can antiquate currently used methods or tools	• Proposed process models risk sub-optimization occurring when only considering least cost manufacturing
• Commercial software packages are costly and fragmented impeding their wide-scale adoptions	• Standards cannot readily address the difficulty of sharing process models and linking them due to process setup variability and machine age

To this end, ASTM International has formed both a committee on Sustainability (E60) and a Subcommittee on Sustainable Manufacturing (E60.13) [52].

Of immediate relevance to this paper is the recently published *E3012-16 Standard Guide for Characterizing Environmental Aspects of Manufacturing Processes*, provides guidance for the actual characterization of manufacturing processes [16]. This guide outlines a characterization methodology and proposes a generic representation from which manufacturers can derive specific UMP representations for meaningful sustainability performance analysis. Also, ASTM published two related standards namely, *E2986-15 Standard Guide for Evaluation of Environmental Aspects of Sustainability of Manufacturing Processes*, which provides guidance for manufacturers on how to conduct a sustainability study in order to improve their practices [15] and *E2987/E2987M-16 Standard Terminology for Sustainable Manufacturing*, includes terminology applicable to sustainable manufacturing [53]. Other relevant standards under development within the E60.13 Subcommittee include:

- Classification for Waste Generated at Manufacturing Facilities,
- Guide for Integration and Reporting of Environmental and Social Sustainability within the Manufacturing Supply Chains,
- Standard Specification for Net-Negative Landfill Waste Manufacturing Processes.

The vision of these standards is to provide manufacturers with a way to better describe their manufacturing processes with regards to sustainability. This will facilitate data exchange, sharing and communication with other manufacturing applications, such as LCA. The ease with which data can be exchanged and compared sets the stage for the development of decision-making tools capable of benchmarking sustainability process performances. These tools access standardized repositories of reusable UMP models.

CONCLUSIONS

With limited resources available and cultures that have yet to become proactive, companies have struggled to implement sustainability initiatives that extend deeply into their operations. In part, this is the result of research advocating the use of many indicators and metrics, without providing easy-to-learn, quality introductory tools or directly equating all metrics to cost values. On the other hand, industry is reluctant to collectively share, even if anonymously, information regarding processes and materials.

The findings from the roundtable meetings indicate a need for metrics that are simple and relate to core business practices, transparent data and information flows, process models that are accessible, accurate, and standardized, and incentives to speed the adoption of these methods. From the results of the roundtables, it is apparent that the development of standards for representing manufacturing processes and collecting relevant sustainability data is both needed and will support industry's ability and desire to collect more accurate data for sustainability assessment. Further, these standards will support the reuse of that data in multiple types of analyses.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.
Approved for public release; distribution is unlimited.

TABLE 2: RECOMMENDED CHANGES TO CURRENT PRACTICES TO FACILITATE ADOPTION OF STANDARDS

Manufacturing Metrics & Measurements	
• Orient standard metrics to explicitly state cost value to appeal to high level management who are chiefly concerned with maintain cost competitiveness and market share • Make metrics and indicators standard industry wide to facilitate friendly competition and increase supplier participation • Make tools with an easy entry version to highlight small improvements and aid in identifying low hanging fruit and to justify larger investments • Any sustainable manufacturing tool should be usable on current equipment (e.g., machine tools) to demonstrate future usefulness • Incorporate traceability into sustainable manufacturing tools as it is frequently requested by manufacturers • Clearly and uniformly define tool boundaries and capabilities to reassure industry that they are purchasing and using the correct tool • Identify environmental impact drivers using on-the-line data and not industry or facility averages	• Due to the high cost of creating full manufacturing process models, create a "light" version focusing only on primary process drivers to alleviate initial investment concerns • Develop a library of materials and UMPs to aid design-for-manufacture decision making and to be incorporated into the engineering toolbox • Engage shop floor personnel by showing real-time feedback on the sustainability performance metrics through visualizations, such as dashboards • Incorporate process modeling into the manufacturing step of LCA to increase total model accuracy and identify areas for improvements • Plan for the introduction of new top-down regulations and their impact on product manufacturing • Demonstrate an allocation method for system-level indicators, such as how occupational health and safety information is directly relatable to product manufacture • Incorporate accountability of materials and consumables into assessments e.g., including impact of an alternative solvent within an LCA
Manufacturing Process Modeling	
• Consider regional location, access to resources, and laws when conducting LCAs and developing process models. No standard as of yet allows a large degree of localization freedom or adaptability • Future standards development should integrate UMP models back into LCA methods and tools	• Make models and data generated by a standard or government accessible to all e.g., integrate with the Digital Commons or the NREL U.S. Life Cycle Inventory Database • Standardize the composability of UMP models such that they do not require soliciting the individuals who created the process models to understand the underlying process models

Future work will involve the deployment of the proposed standards for sustainable manufacturing. Pilot projects in specific industries will serve to validate the standards and their usability, utility, and benefits. Projects will be designed to address a chosen problem within a company and apply the new standards to facilitate the problem definition and data collection. The standards [16][15] shall guide the user through selecting a goal, choosing relevant indicators, assigning process boundaries, identifying process metrics, and determining the input-output transformations. Experience gained from the completion of pilot projects will influence future editions of the standard. Further, the pilot projects will lay the foundation for exploring composability of UMP models.

Composability is an ongoing area of research into modeling how UMPs meaningfully interact and link together within manufacturing systems [35,54]. The suggestions and barriers identified in the dialogues support the reasoning that standards are needed to assist in the composition of the process models such that process-level issues can be holistically evaluated and mapped to the system-level decision making. Future work and standards development will involve developing tools and methods capable of assessing the sustainability of manufacturing systems. This system should be supported by information models that standardize the relationships between UMPs [55], which would further the goal of integrating sustainability into manufacturing system performance decisions [56].

ACKNOWLEDGMENTS

The authors gratefully acknowledge the National Institute of Standards and Technology (NIST Award No. 70NANB13H155), especially Kevin Lyons, Simon Frechette, and Swee Leong, for support of this research, and the assistance of Dr. Jacqueline Isaacs and Dr. Pei Zhai (Northeastern University) and Ian Garretson and Harsha Malshe (Oregon State University) in roundtable organization and data collection/interpretation.

DISCLAIMER

No approval or endorsement of any commercial product by the National Institute of Standards and Technology is intended or implied. Certain commercial software systems are identified in this paper to facilitate understanding. Such identification does not imply that these software systems are necessarily the best available for the purpose.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.
Approved for public release; distribution is unlimited.

Mani, Mahesh; Haapala, Karl; Smullin, Matteo; Morris, Katherine. SP-625
"Using Industry Focus Groups and Literature Review to Identify Challenges in Sustainable Assessment Theory and Practice."
Paper presented at the ASME International Design Engineering Technical Conference, Charlotte, NC, Aug 21-Aug 24, 2016.

REFERENCES

[1] USDOC, 2011, “How does Commerce define Sustainable Manufacturing?,” Int. Trade Adm. US Dep. Commer. [Online]. Available: http://trade.gov/competitiveness/sustainablemanufacturing/how_doc_defines_SM.asp. [Accessed: 30-Dec-2012].

[2] Fan, C., Carrell, J. D., and Zhang, H.-C., “An Investigation of Indicators for Measuring Sustainable Manufacturing.”

[3] Joung, C. B., Carrell, J., Sarkar, P., and Feng, S. C., 2013, “Categorization of Indicators for Sustainable Manufacturing,” Ecol. Indic., **24**, pp. 148–157.

[4] Singh, R. K., Murty, H. R., Gupta, S. K., and Dikshit, A. K., 2012, “An Overview of Sustainability Assessment Methodologies,” Ecol. Indic., **15**(1), pp. 281–299.

[5] Allen, D., Bauer, D., Bras, B., Gutowski, T., Murphy, C., Piwonka, T., Sheng, P., Sutherland, J., Thurston, D., and Wolff, E., 2002, “Environmentally Benign Manufacturing: Trends in Europe, Japan, and the USA,” J. Manuf. Sci. Eng., **124**(4), pp. 908–920.

[6] Bunse, K., Vodicka, M., Schönsleben, P., Brülhart, M., and Ernst, F. O., 2011, “Integrating energy efficiency performance in production management – gap analysis between industrial needs and scientific literature,” J. Clean. Prod., **19**(6–7), pp. 667–679.

[7] Bhanot, N., Rao, P. V., and Deshmukh, S. G., 2015, “Enablers and Barriers of Sustainable Manufacturing: Results from a Survey of Researchers and Industry Professionals,” Procedia CIRP, **29**, pp. 562–567.

[8] Rachuri, S., Sriram, R. D., and Sarkar, P., 2009, “Metrics, Standards and Industry Best Practices for Sustainable Manufacturing Systems,” 5th Annual IEEE Conference on Automation Science and Engineering, Bangalore, India, pp. 472–477.

[9] Ryan, F., Coughlan, M., and Cronin, P., 2008, “Undertaking a literature review: a step-by-step approach,” Sch. Nurs. Midwifery Trinity Coll. Dublin.

[10] Webster, J., and Watson, R., 2002, “Analyzing the Past to Prepare for the Future: Writing a Literature Review,” MIS Q., **26**(2), pp. xiii–xxiii.

[11] Audretsch, D. B., and Feldman, M. P., 1996, “R&D spillovers and the geography of innovation and production,” Am. Econ. Rev., pp. 630–640.

[12] Ven, A. H. V. D., and Delbecq, A. L., 1974, “The Effectiveness of Nominal, Delphi, and Interacting Group Decision Making Processes,” Acad. Manage. J., **17**(4), pp. 605–621.

[13] Okoli, C., and Pawlowski, S. D., 2004, “The Delphi method as a research tool: an example, design considerations and applications,” Inf. Manage., **42**(1), pp. 15–29.

[14] Stewart, D. W., Shamdasani, P. N., and Rook, D., 2006, Focus Groups: Theory and Practice, SAGE Publications, Inc.

[15] ASTM E2986-15, 2015, Standard Guide for Evaluation of Environmental Aspects of Sustainability of Manufacturing Processes, ASTM International.

[16] ASTM E3012-16, 2016, Standard Guide for Characterizing Environmental Aspects of Manufacturing Processes, ASTM International.

[17] Baumann, H., and Rydberg, T., 1994, “Life cycle assessment: A comparison of three methods for impact analysis and evaluation,” J. Clean. Prod., **2**(1), pp. 13–20.

[18] Azapagic, A., and Clift, R., 1999, “The application of life cycle assessment to process optimisation,” Comput. Chem. Eng., **23**(10), pp. 1509–1526.

[19] Krajnc, D., and Glavič, P., 2005, “How to Compare Companies on Relevant Dimensions of Sustainability,” Ecol. Econ., **55**, pp. 551–563.

[20] Smith, L., and Ball, P., 2012, “Steps towards sustainable manufacturing through modelling material, energy and waste flows,” Int. J. Prod. Econ., **140**(1), pp. 227–238.

[21] Zhang, H., and Haapala, K. R., 2012, “Integrating Sustainability Assessment into Manufacturing Decision Making,” Leveraging Technology for a Sustainable World, D.A. Dornfeld, and B.S. Linke, eds., Springer Berlin Heidelberg, pp. 551–556.

[22] Linke, B. S., Corman, G. J., Dornfeld, D. A., and Tönissen, S., 2013, “Sustainability Indicators for Discrete Manufacturing Processes Applied to Grinding Technology,” J. Manuf. Syst., **32**(4), pp. 556–563.

[23] Linke, B., Das, J., Lam, M., and Ly, C., 2014, “Sustainability Indicators for Finishing Operations based on Process Performance and Part Quality,” Procedia CIRP, **14**, pp. 564–569.

[24] Diaz-Elsayed, N., Dornfeld, D., and Horvath, A., 2015, “A comparative analysis of the environmental impacts of machine tool manufacturing facilities,” J. Clean. Prod., **95**, pp. 223–231.

[25] Ahi, P., and Searcy, C., 2015, “An analysis of metrics used to measure performance in green and sustainable supply chains,” J. Clean. Prod., **86**, pp. 360–377.

[26] Chen, D., Thiede, S., Schudeleit, T., and Herrmann, C., 2014, “A holistic and rapid sustainability assessment tool for manufacturing SMEs,” CIRP Ann. - Manuf. Technol., **63**(1), pp. 437–440.

[27] Shelton, J. D., 2010, “An investigation of sustainability metrics in industry to aid product design, production, and distribution processes,” Doctoral Dissertation, The Pennsylvania State University.

[28] Labuschagne, C., Brent, A. C., and van Erck, R. P. G., 2005, “Assessing the sustainability performances of industries,” J. Clean. Prod., **13**(4), pp. 373–385.

[29] Baumgartner, R. J., and Ebner, D., 2010, “Corporate sustainability strategies: sustainability profiles and maturity levels,” Sustain. Dev., **18**(2), pp. 76–89.

[30] Gunasekaran, A., and Spalanzani, A., 2012, “Sustainability of manufacturing and services: Investigations for research and applications,” Int. J. Prod. Econ., **140**(1), pp. 35–47.

[31] Eastwood, M. D., and Haapala, K. R., 2015, “A Unit Process Model Based Methodology to Assist Product

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.
Approved for public release; distribution is unlimited.

Sustainability Assessment During Design for Manufacturing," J. Clean. Prod., **108**, **part A**, pp. 54–64.

[32] Kellens, K., 2013, "Energy and Resource Efficient Manufacturing - Unit Process Analysis and Optimization," Doctoral Dissertation, University of Leuven.

[33] Dixit, U. S., Joshi, S. N., and Davim, J. P., 2011, "Incorporation of Material Behavior in Modeling of Metal Forming and Machining Processes: A Review," Mater. Des., **32**(7), pp. 3655–3670.

[34] Eastlick, D. D., and Haapala, K. R., 2012, "Increasing the Utility of Sustainability Assessment in Product Design," ASME 2012 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference, Chicago, IL, pp. 713–722.

[35] Garretson, I. C., 2015, "A Unit Manufacturing Process Characterization Methodology and Supporting Terminology for Sustainable Manufacturing Assessment," Master of Science, Oregon State University.

[36] Munoz, A. A., and Sheng, P., 1995, "An Analytical Approach for Determining the Environmental Impact of Machining Processes," J. Mater. Process. Technol., **53**(3–4), pp. 736–758.

[37] Gutowski, T., Dahmus, J., and Thiriez, A., 2006, "Electrical Energy Requirements for Manufacturing Processes," 13th CIRP International Conference on Life Cycle Engineering, CIRP International, Leuven, Belgium.

[38] Li, W., and Kara, S., 2011, "An empirical model for predicting energy consumption of manufacturing processes: a case of turning process," Proc. Inst. Mech. Eng. Part B J. Eng. Manuf., **225**(9), pp. 1636–1646.

[39] Duflou, J. R., Kellens, K., and Dewulf, W., 2011, "Unit Process Impact Assessment for Discrete Part Manufacturing: A State of the Art," CIRP J. Manuf. Sci. Technol., **4**(2), pp. 129–135.

[40] Overcash, M., and Twomey, J., 2012, "Unit Process Life Cycle Inventory (UPLCI) – A Structured Framework to Complete Product Life Cycle Studies," Leveraging Technology for a Sustainable World, D.A. Dornfeld, and B.S. Linke, eds., Springer Berlin Heidelberg, pp. 1–4.

[41] Kellens, K., Yasa, E., Renaldi, R., Dewulf, W., Kruth, J.-P., and Duflou, J., 2011, "Energy and Resource Efficiency of SLS/SLM Processes," Proceedings of the Solid Freeform Fabrication Symposium, University of Texas, Austin, pp. 1–16.

[42] Murray, V. R., Zhao, F., and Sutherland, J. W., 2012, "Life cycle analysis of grinding: a case study of non-cylindrical computer numerical control grinding via unit-process life cycle inventory approach," Proc. Inst. Mech. Eng. Part B J. Eng. Manuf., p. 954405412454102.

[43] Madan, J., Mani, M., and Lyons, K., 2013, "Characterizing Energy Consumption of the Injection Molding Process," ASME 2013 Manufacturing Science and Engineering Conference, Madison, WI.

[44] Nannapaneni, S., Mahadevan, S., and Rachuri, S., 2016, "Performance evaluation of a manufacturing process under uncertainty using Bayesian networks," J. Clean. Prod., **113**, pp. 947–959.

[45] Tu, Q., and McDonnell, B. E., 2016, "Monte Carlo analysis of life cycle energy consumption and greenhouse gas (GHG) emission for biodiesel production from trap grease," J. Clean. Prod., **112**, **Part 4**, pp. 2674–2683.

[46] Kremer, G. E., Haapala, K., Murat, A., Chinnam, R. B., Kim, K., Monplaisir, L., and Lei, T., 2016, "Directions for instilling economic and environmental sustainability across product supply chains," J. Clean. Prod., **112**, **Part 3**, pp. 2066–2078.

[47] Helu, M., Behmann, B., Meier, H., Dornfeld, D., Lanza, G., and Schulze, V., 2012, "Impact of green machining strategies on achieved surface quality," Cirp Ann.-Manuf. Technol., **61**(1), pp. 55–58.

[48] Aurich, J. C., Linke, B., Hauschild, M., Carrella, M., and Kirsch, B., 2013, "Sustainability of abrasive processes," CIRP Ann. - Manuf. Technol., **62**(2), pp. 653–672.

[49] Tan, H. X., Yeo, Z., Ng, R., Tjandra, T. B., and Song, B., 2015, "A Sustainability Indicator Framework for Singapore Small and Medium-Sized Manufacturing Enterprises," Procedia CIRP, **29**, pp. 132–137.

[50] Vermeulen, W. J. V., and Kok, M. T. J., 2012, "Government interventions in sustainable supply chain governance: Experience in Dutch front-running cases," Ecol. Econ., **83**, pp. 183–196.

[51] Čuček, L., Klemeš, J. J., and Kravanja, Z., 2012, "A Review of Footprint Analysis Tools for Monitoring Impacts on Sustainability," J. Clean. Prod., **34**, pp. 9–20.

[52] "Subcommittee E60.13 on Sustainable Manufacturing" [Online]. Available: http://www.astm.org/COMMIT/SUBCOMMIT/E6013.htm.

[53] ASTM E2987/E2987M-16, 2016, Standard Terminology for Sustainable Manufacturing, ASTM International.

[54] Mani, M., Madan, J., Lee, J. H., Lyons, K. W., and Gupta, S. K., 2014, "Sustainability Characterization for Manufacturing Processes," Int. J. Prod. Res., **52**(20), pp. 1–18.

[55] Witherell, P., Feng, S., Simpson, T. W., Saint John, D. B., Michaleris, P., Liu, Z.-K., Chen, L.-Q., and Martukanitz, R., 2014, "Toward Metamodels for Composable and Reusable Additive Manufacturing Process Models," J. Manuf. Sci. Eng., **136**(6), pp. 061025–061025.

[56] AlKhazraji, Q. Y., Saldana, C., Donghuan, T., and Kumara, S., 2013, "Information modeling to incorporate sustainability into production plans," 2013 IEEE International Conference on Automation Science and Engineering (CASE), pp. 516–521.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.
Approved for public release; distribution is unlimited.

Technical Report: Towards a Systematic Threat Modeling Approach for Cyber-physical Systems

Goncalo Martins[1], Sajal Bhatia[1], Xenofon Koutsoukos[1], Keith Stouffer[2], CheeYee Tang[2], and Richard Candell[2]

[1]Institute for Software Integrated Systems (ISIS), Department of Electrical Engineering and Computer Science
Vanderbilt University, Nashville, Tennessee, USA
Goncalo.Martins@vanderbilt.edu
Sajal.Bhatia@vanderbilt.edu
Xenofon.Koutsoukos@vanderbilt.edu
[2]National Institute of Standards and Technology (NIST)
Gaithersburg, Maryland, USA
Keith.Stouffer@nist.gov
CheeYee.Tang@nist.gov
Richard.Candell@nist.gov

***Abstract*—Cyber-Physical Systems (CPS) are systems that integrate physical, computational, and networking components. These systems have an impact on the physical components; it is critical to safeguard them against a range of attacks. In this paper, it is argued that an effective approach to achieve this goal is to systematically identify the potential threats at the design phase of building such systems, commonly achieved via threat modeling. In this context, a tool to perform systematic analysis of threat modeling for CPS is proposed. A real-world wireless railway temperature monitoring system is used as a case study to validate the proposed approach. The threats identified in the system are subsequently mitigated using the National Institute of Standards and Technology (NIST) SP 800-82 guidelines.**

***Keywords*-Threat Modeling, Systematic Analysis, Cyber-Physical Systems, Case Study**

I. Introduction

The exponential growth of information and communication technologies over the last decade has given rise to their expansion in real-world applications involving physical processes. This expansion has led to the emergence of closed-loop systems involving strong integration and coordination of physical and cyber (computational and communication) components, often referred to as Cyber-Physical Systems (CPS). These systems are rapidly finding their way into various aspects of the contemporary society such as transportation, healthcare, and critical infrastructure. Increasing dependence on CPS and their potential effects on the physical world, demands them to be inevitably secure, robust, reliable, and trustworthy. Ironically, it also makes such systems very attractive targets for ever increasing, both in number and complexity, cyber attacks.

The complex nature of CPS makes securing such systems go beyond securing each of these components in isolation. A multi-vector attack, exploiting a combined set of vulnerabilities from each of these individual components, can have damaging effects. A prominent recent example of such multi-vector attack was the Stuxnet attack that targeted nuclear centrifuges at the Iranian uranium enrichment plant [1]. In this attack, a worm propagating via Universal Serial Bus (USB) and local network, exploited a zero-day vulnerability of Windows machines and thereby infected the Programmable Logic Controllerss (PLCs). Another example of a multi-vector attack was the Slammer SQL worm which infected a private network at the Davis-Besse nuclear power station and resulted in a substantial time loss of safety monitoring systems [2].

Efforts in securing these CPS have mainly been towards extending the existing approaches to secure their individual components – cyber and physical. This paper, however, argues that it is imperative to simultaneously consider both these components to achieve the desired security of such systems. This goal can be achieved by identifying potential vulnerabilities of such systems, preferably during the design-phase, to minimize the overall costs involved in providing and maintaining their security and reliability. One of the ways in which this identification can be performed is *threat modeling*. In this context, various approaches have been proposed in the literature. Attack tree based approaches [3] are widely used mainly due to their simplistic design. However, static nature and state space explosion considerably restricts their modeling capabilities. Moreover, the reviewed literature also indicates a scarcity of systematic threat modeling approaches and software tools that can be used to perform a comprehensive analysis of a wide range of threats to a variety of CPS. This paper addresses these limitations and it makes the following key contributions.

Martins, Goncalo; Bhatia, Sajal; Koutsoukos, Xenofon; Stouffer, Keith; Tang, CheeYee; Candell, Richard. "Towards a Systematic Threat Modeling Approach for Cyber-physical Systems." Paper presented at the National Symposium on Resilient Critical InFrastructure (ISRCS), Philadelphia, PA, Aug 18-Aug 20, 2015.

- Presents a tool to perform systematic threat modeling for CPS using a real-world railway temperature monitoring system as the case study.
- Identifies threats and the corresponding mitigation using the National Institute of Standards and Technology (NIST) guidelines [4].

Another contribution of this work is the adaptation of Microsoft's Security Development Lifecycle (SDL) Threat Modeling Tool [5] for threat identification in the CPS domain. Currently, the SDL tool can be used for analyzing threats in web applications. The paper models software-related threats within the CPS domain in a systematic manner. Modeling of hardware-related threats and combining them with currently identified software-related threats constitutes a part of the future research work in this direction.

The remainder of the paper is organized as follows: Section II gives an overview of the related work in the area of threat modeling. This section also outlines the security guidelines from NIST used to address the threat identified in the case study. Section III discusses the modeling paradigm, including the metamodel and interpreters, developed for this work. Section IV describes the case study used in this paper. This section also presents the resulting modeling environment, threats identified, and addressed using NIST standards. Finally, Section V summarizes the work and gives directions for future work in this area.

II. Background and Related Work

A. Threat Modeling

Threat modeling is an approach for analyzing the security of an application. It is a structured approach that allows a systematic identification and rating of all the security-related threats that are most likely to affect the system under consideration.

Threat modeling is based on a comprehensive understanding of the underlying architecture and implementation details of the system; and provides a way to address these identified threats with appropriate countermeasures. During threat modeling, two types of models are commonly used: a model of what it is being built, and a model of the threats.

For threat models, an approach centered on asset models, attacker models, or software models is used. It is more beneficial to model threats using an individual approach at the time rather than to combine all the models [5].

The attacker-centric approach focuses on identifying the attacker, evaluating their goals, and attempting to predict how these goals might be achieved by the attacker. Software-centric threat modeling, also referred to as system-centric, design-centric, or architecture-centric, begins with the design model of the system under consideration. It focuses on all possible attacks that target each of the model elements. The asset-centric approach focuses on all the individual assets (a system or user level resource associated with certain value) entrusted to the system.

The author in [5] points out the advantages and disadvantages of assets models, attacker models, and software models. However, one of the strong motivations to apply software models for threat modeling relies on software being the foundation of any application, which makes it an ideal place to start the threat-modeling task. Moreover, almost all software development is done with software models that help understand the application. Developers are encouraged to make them good enough to allow effective threat modeling.

B. Threat Modeling Approaches

A majority of existing approaches for threat modeling can be broadly divided into two main groups – attack tree-based approaches and stochastic model-based approaches.

Attack tree-based modeling was presented in [3]. Attack trees formally describe the security of the system under consideration against a variety of attacks. They represent all possible attacks against a system in a tree structure, with the root node representing the overall goal of the attack and leaf nodes representing the different ways of achieving that goal.

Attack trees have been used in a variety of applications. Fung et al. [6] used attack trees to model three fundamental security mechanisms – confidentiality, integrity, and availability of MANET networks. Higuero et al. [7] used attack trees to model digital content security. Bistarelli et al. [8] proposed an extension to attack trees that incorporated defense mechanisms against intrusions on leaf nodes, which they termed as defense trees. This work was further extended by Kordy et al. [9] by formally introducing an attack-defense tree (ADTree). ADTrees not only took into account measures taken by an attacker to compromise a system but also incorporated defense mechanisms employed by a defender to protect the system.

Stochastic model-based threat modeling approaches commonly convert system models to Markov chains and analyze them using state transition matrices. This approach was used by Madan et al. [10] to conduct behavioral analysis of a intrusion tolerant system. Sallhammar et al. [11] presented an integrated security and dependability evaluation approach based on stochastic modeling using game theory to model attackers' behavior. Even though stochastic modeling-based approaches provide stronger and more formal modeling power than attack tree-based approaches, lack of precise representation of an attackers behavior to known distribution functions used in such models limits their usability.

C. Threat Modeling for CPS

This section outlines some of threat modeling techniques that have been applied to the CPS domain. Yampolskiy et al. [12] assessed the applicability of a data flow diagram (DFD) based approach for systematically analyzing cyber-attacks on CPS. In this context, [12] proposed a number of extensions to DFD and evaluated their proposed approach using a quad-rotor unmanned aerial vehicle (UAV) as a case study. The security assessment approach presented by the authors was manual in nature and was strongly dependent on the knowledge-base of the domain expert. Zalewski et al. [13] used Discrete Time Markov Chains (DTMC) to obtain state change (from secure to insecure) probabilities of security violations of a Cooperative Adaptive Cruise Control (CACC) system (considered a CPS system). The authors analyzed and compared two methods (Damage, Reproducibility, Exploitability, Affect Users, and Discoverability (DREAD) model [14] and Common Vulnerability Scoring System (CVSS) base metric [15]) of threat modeling of an inter vehicular communication (IVC) system using Microsoft's SDL threat modeling tool [5]. The authors in [13] acknowledged that both of the methods were developed for security analysis of Internet based applications and may not be directly applicable to CPS domain.

CPS are a combination of hardware and software modules; security of these systems is still in its infancy. To the best of our knowledge, there aren't any publicly available tools (or techniques) that automatically perform a systematic analysis of security threats in the CPS domain. As previously mentioned, it is believed that an automated hardware and software threat modeling approach, done in the design stage of the system, can help find potential problems that with other approaches would be hard or even impossible to cover.

D. Systems Security Standards

This section describes the standard document, NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security* [4]. This document provides guidance for establishing system security for industrial control systems (ICS). It provides a notional overview of ICS, reviews typical system topologies and architectures, identifies known threats and vulnerabilities to the ICS systems, and provides recommended security countermeasures to mitigate the associated risks. This document established a framework and process to provide guidance to perform risk assessment, security program development and deployment, and to apply security controls to ICS.

It covers the security controls in the following families: Access Control; Awareness and Training; Audit and Accountability; Security Assessment and Authorization; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Planning; Personnel Security; Risk Assessment; System and service Acquisition; System and Communications Protection; and System and Information Integrity.

III. Modeling Paradigm by Domain

As mentioned in Section II, the number of available tools that allow a systematic analysis of threats for CPS is scarce. The scarcity of tools is dependent upon the heterogeneous features of such systems. CPS are composed of hardware and software elements which makes it challenging to model all the security requirements in one tool. To address this challenge, the Generic Modeling Environment (GME) [16] used to support the creation of domain-specific modeling for threat analysis on CPS is proposed.

GME allows the design of metamodels specifying the modeling language of the application domain. The modeling language contains all the syntactic, semantic, and presentation information regarding the domain. Moreover, the modeling language defines the family of models that can be created using the resultant modeling environment.

The proposed modeling paradigm consists of applying and extending the SDL threat modeling tool [5] to model, identify, and mitigate threats in a systematic way for the proposed CPS (Section IV).

A. Metamodel

The first step of developing a metamodel consists of defining a sketch of a metamodel for threat analysis for the proposed CPS. This is achieved by using the MetaGME modeling language, which is installed and registered by default in GME. MetaGME is basically a Unified Modeling Language (UML) Class Diagram extended with some additional concepts, including Object Constraint Language (OCL) constraints and configurable visualization properties.

The CPS components from Section IV are modeled as *first class objects* (FCOs) in GME. The defined FCOs contain both textual Attributes and Constraints. The textual Attributes are related with security aspects from the SDL threat modeling tool (e.g., authentication mechanism attribute). The Constraints are OCL-based expressions to enable verifiability for the models.

Figure 1 presents the metamodel for the proposed CPS model domain. It consist of four FCOs (sensor, repeater, gateway and central station), and two types of connections (WiFi 2.4 GHz and wireless 868 MHz). For this case-study, the components are modeled as processes from the DFD defined in the SDL threat modeling tool. The DFD process attributes were incorporated in the metamodel by implementing them as textual attributes. Figure 2 shows an example of the attributes implemented for data flow connections in GME.

B. Interpreters

One of the motivations for modeling threats in GME is the desire to describe a system in a structured way and to use the description as a form of identifying threats in a systematic way. Moreover, we also want to analyze the model automatically. Typically, the model analyzes range from simple to sophisticated:

- running queries, generating lists, and writing reports based on the contents of the model;
- generating program code or system configuration;

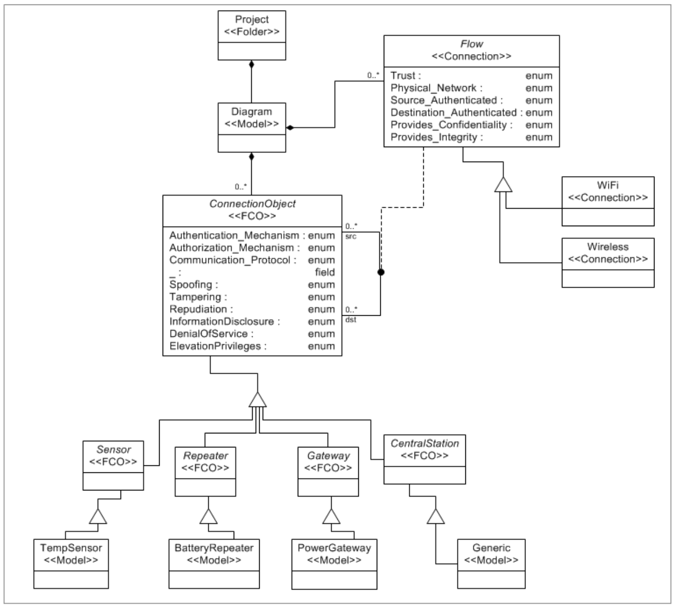


Figure 1. GME metamodel - case study

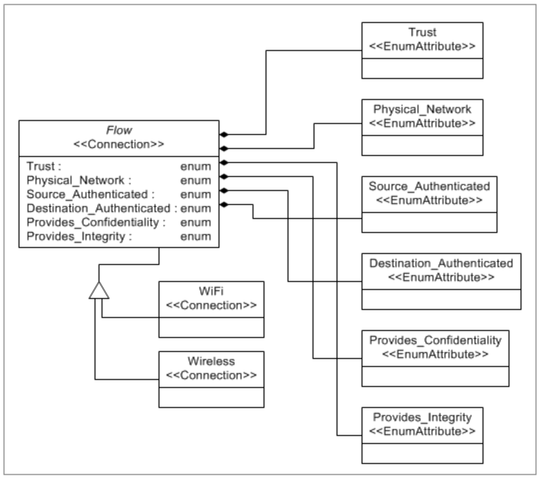


Figure 2. GME metamodel - Data Flow Connection Attributes

- using the models as a data exchange format to integrate tools that are incompatible with each other.

To perform the model analysis, programmatic access to the GME model information is required. To meet this requirement, we are using a technique provided by GME called interpreters. Interpreters are not standalone programs; they are components (usually dynamic link libraries (DLLs)) that are loaded and executed by GME upon a user's request. In this case, we developed the interpreter code responsible for navigating through the model, analyzing the results and extracting the security vulnerabilities present in all data flow connections. The security vulnerabilities are the same as the ones identified in the SDL threat modeling tool, with the exception that in this case the vulnerabilities are adapted and related to the CPS case-study system.

IV. Case Study: eRTM

The CPS case study consists of a wireless sensor network for monitoring of rail temperature[1] (eRTM system). A possible eRTM system architecture is presented in Figure 3 and consists of two main sections: a CPS system section and an Internet Protocol (IP) network section.

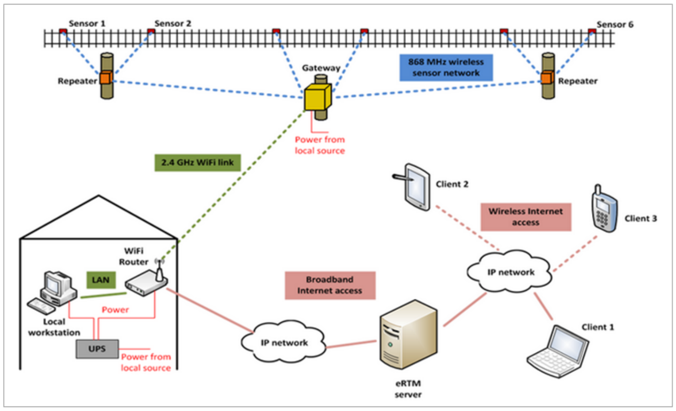


Figure 3. eRTM Generic System Architecture[1]

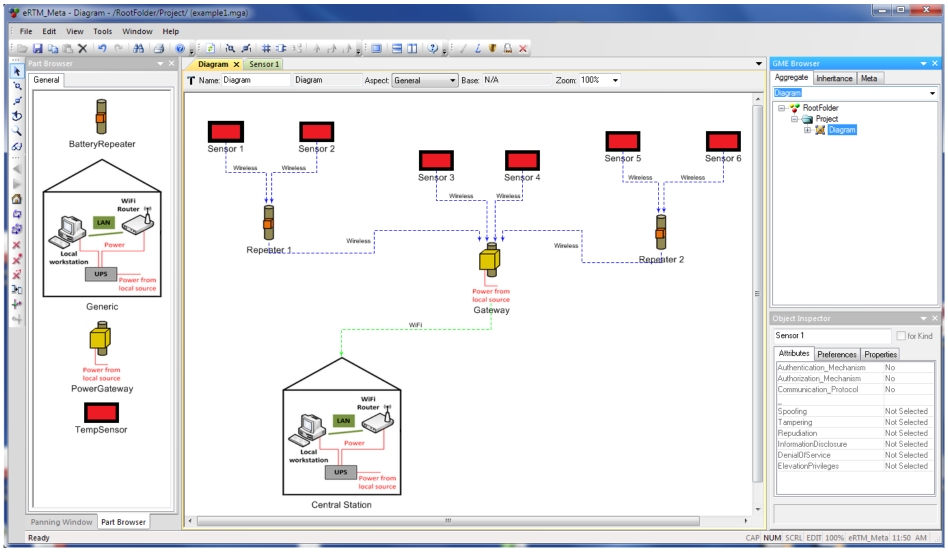
The CPS system section is comprised of battery-powered temperature-measuring modules (sensors) connected via 868 MHz radio channels. These sensors gather temperature-related information and communicate it to the gateway units via the repeaters. These gateway units subsequently transmit all the collected information to a central station through a 2.4 GHz WiFi link. The processed monitoring information is then communicated to clients via the conventional IP network and is made accessible through browsers and smartphone applications. Based on the temperature limit settings, alarm messages are sent to specified clients. This work covers only the CPS system section of Figure 3.

A. Resultant Modeling Environment

1) System Model: The CPS system components from Figure 3 are modeled in GME. The resultant modeling environment is presented in Figure 4. Table I summarizes the selected model properties for the components present in the modeling environment. The model properties used for each component are the following: code type, which can be native or managed; running code as, either administrator or local user; and accepts inputs, from nothing or any remote user or entity.

2) Finding Threats: There are nine data flow connections and after running the interpreter described in Section III-B, the modeling environment identified ten threats for each data flow (a total of 90 threats).

[1] http://www.evopro.hu/eng/page/ertm



Name: Diagram | Diagram | Aspect: General | Base: N/A | Zoom: 100%

Object Inspector: Sensor 1 □ for Kind

Attributes | Preferences | Properties

Authentication_Mechanism	No
Authorization_Mechanism	No
Communication_Protocol	No
_	
Spoofing	Not Selected
Tampering	Not Selected
Repudiation	Not Selected
InformationDisclosure	Not Selected
DenialOfService	Not Selected
ElevationPrivileges	Not Selected

Figure 4. GME eRTM Model

Table I
MODEL PROPERTIES

Component	# Components	Model Properties		
Sensor	6	Code Type: Managed	Running As: Administrator	Accepts Input From: Nothing
Gateway	1	Code Type: Managed	Running As: Administrator	Accepts Input From: Any Remote User or Entity
Repeater	2	Code Type: Managed	Running As: Administrator	Accepts Input From: Any Remote User or Entity
Central Station	1	Code Type: Managed	Running As: Administrator	Accepts Input From: Any Remote User or Entity
WiFi	1	Physical Network: 2.4 GHz	Trust: No	
Wireless	8	Physical Network: 868 MHz	Trust: No	

As an example, two Spoofing threats, one Tampering threat, one Repudiation threat, one Information Disclosure threat, two Denial Of Service threats, and three Elevation Of Privileges threats were identified between a Sensor and a Repeater. Table II summarizes these ten threats.

3) Addressing Threats: Based on the security categorization process, the security control baseline for the eRTM case study was categorized as a moderate impact system, as the impact on confidentiality is low, and the impact on integrity and availability are both moderate [4].

According to SP 800-82 Appendix G, ICS Overlay, all security controls for the moderate baseline should be implemented. However, for the illustration purpose of this case study, certain controls are selected to directly address the threat identified by the threat modeling tool, as summarized in Table II.

V. Conclusion and Future Work

The complex nature of CPSs makes securing such systems a challenge. Efforts in securing CPSs have mainly been focused towards extending the existing approaches to secure their individual components - cyber and physical. However, it is important to identify the potential vulnerabilities during the design-phase in a systematic way to minimize the overall costs involved in providing and maintaining their security and reliability. This paper addresses these challenges by proposing a tool that allows, during a CPS design phase, a systematic analysis of threat modeling for a CPS using a real-world railway temperature monitoring system as the case study. After identifying the possible threats in the modeled CPS system, the proposed approach also addresses them using the NIST security guidelines.

There are two main directions as future work: first, CPS systems are a combination of software and hardware components. To date, the proposed tool only addresses software threats. The combination and/or correlation of software and hardware threats needs to be investigated. The authors will explore the feasibility of including hardware threats in the existing modeling environment. Second, there is more than one way to do threat modeling, and the best way to threat modeling is the way that allows one to find more threats against a system. The authors will investigate ways to merge different threat modeling techniques (e.g., attack tree-based approaches) with the proposed one to enable the expansion of threat identification and system vulnerabilities.

VI. Acknowledgments

This work was supported in part by NIST (70NANB13H169), the National Science Foundation under Award CNS-1238959, and by the Air Force Research Laboratory under Award FA8750-14-2-0180.

VII. Disclaimer

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not

Table II
IDENTIFIED THREATS AND RESPECTIVE MITIGATION BETWEEN A SENSOR AND A REPEATER

Threat	Description	Mitigation Control Number	Mitigation Control Name
1. Elevation Using Impersonation	Repeater may be able to impersonate the context of Sensor in order to gain additional privilege.	IA-3 (1) (4)	Device Identification and Authentication
2. Spoofing the Sensor	Sensor may be spoofed by an attacker and this may lead to unauthorized access to Repeater.	SC-7 (3) (4) (5) (7) (18) SC-8 (1)	Boundary Protection Transmission Confidentiality and Integrity
3. Spoofing the Repeater	Repeater may be spoofed by an attacker and this may lead to information disclosure by Sensor.	SC-7 (3) (4) (5) (7) (18) SC-8 (1)	Boundary Protection Transmission Confidentiality and Integrity
4. Potential Lack of Input Validation for Repeater	Data flowing across 868 MHz Wireless may be tampered with by an attacker.	SI-10	Information Input Validation
5. Potential Data Repudiation by Repeater	Repeater claims that it did not receive data from a source outside the trust boundary.	AU-8 (1) AU-9 (4)	Time Stamps Protection of Audit Information
6. Data Flow Sniffing	Data flowing across 868 MHz Wireless may be sniffed by an attacker.	SC-7 (3) (4) (5) (7) (18) SC-8 (1)	Boundary Protection Transmission Confidentiality and Integrity
7. Potential Process Crash or Stop for Repeater	Repeater crashes, halts, stops or runs slowly; in all cases violating an availability metric.	SC-5 SC-6	Denial of Service Protection Resource Availability
8. Data Flow 868 MHz Wireless Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	SC-5 SC-7 (3) (4) (5) (7) (18) SC-8 (1)	Denial of Service Protection Boundary Protection Transmission Confidentiality and Integrity
9. Repeater May be Subject to Elevation of Privilege Using Remote Code Execution	Sensor may be able to remotely execute code for Repeater.	IA-3 (1) (4) SC-7 (3) (4) (5) (7) (18) SC-8 (1) SI-7 PE-4	Device Identification and Authentication Boundary Protection Transmission Confidentiality and Integrity Software, Firmware, and Information Integrity Access Control for Transmission Medium
10. Elevation by Changing the Execution Flow in Repeater	An attacker may pass data into Repeater in order to change the flow of program execution within Repeater to the attacker's choosing.	IA-3 (1) (4) SC-7 (3) (4) (5) (7) (18) SC-8 (1) SI-7 PE-4	Device Identification and Authentication Boundary Protection Transmission Confidentiality and Integrity Software, Firmware, and Information Integrity Access Control for Transmission Medium

intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

REFERENCES

[1] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, 2011.

[2] E. Levy, "Crossover: online pests plaguing the off line world," *Security & Privacy, IEEE*, vol. 1, no. 6, pp. 71–73, 2003.

[3] B. Schneier, "Attack trees: modeling security threats," 1999.

[4] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, "NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security," tech. rep., National Institute of Standards and Technology, 2014.

[5] A. Shostack, *Threat Modeling, Designing for Security*. Wiley, 2014.

[6] C. Fung, A. Chen, X. Wang, J. Lee, R. Tarquini, M. Anderson, and R. Linger, "Survivability analysis of distributed systems using attack tree methodology," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, pp. 583–589, IEEE, 2005.

[7] M. Higuero, J. Unzilla, E. Jacob, P. Saiz, M. Aguado, and D. Luengo, "Application of'attack trees' in security analysis of digital contents e-commerce protocols with copyright protection," in *Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on*, pp. 57–60, IEEE, 2005.

[8] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, pp. 8–pp, IEEE, 2006.

[9] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, "Foundations of attack–defense trees," in *Formal Aspects of Security and Trust*, pp. 80–95, Springer, 2011.

[10] B. B. Madan, K. Gogeva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "Modeling and quantification of security attributes of software systems," in *Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on*, pp. 505–514, IEEE, 2002.

[11] K. Sallhammar, B. E. Helvik, and S. J. Knapskog, "Towards a stochastic model for integrated security and dependability evaluation," in *Availability, Reliability*

and Security, 2006. ARES 2006. The First International Conference on, pp. 8–pp, IEEE, 2006.

[12] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "Systematic analysis of cyber-attacks on cps-evaluating applicability of dfd-based approach," in *Resilient Control Systems (ISRCS), 2012 5th International Symposium on*, pp. 55–62, IEEE, 2012.

[13] J. Zalewski, S. Drager, W. McKeever, and A. J. Kornecki, "Threat modeling for security assessment in cyberphysical systems," *CSIIRW '13 Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, Article No. 10*, 2013.

[14] J. A. Ingalsbe, L. Kunimatsu, T. Baeten, and N. R. Mead, "Threat modeling: diving into the deep end," *Software, IEEE*, vol. 25, no. 1, pp. 28–34, 2008.

[15] P. Mell, K. Scarfone, and S. Romanosky, "A complete guide to the common vulnerability scoring system version 2.0," in *Published by FIRST-Forum of Incident Response and Security Teams*, pp. 1–23, 2007.

[16] A. Ledeczi, M. Maroti, A. Bakay, G. Karsai, J. Garrett, C. Thomason, G. Nordstrom, J. Sprinkle, and P. Volgyesi, "The generic modeling environment," *IEEE International Symposium on Intelligence Signal Processing (WISP), May*, 2001.

STANDARD REFERENCE MATERIALS FOR THE POLYMERS INDUSTRY

Walter G. McDonough, Sara V. Orski, Charles M. Guttman, Kalman D. Migler,
and Kathryn L. Beers, National Institute of Standards and Technology, Gaithersburg, MD

Abstract

The National Institute of Standards and Technology (NIST) provides science, industry, and government with a central source of well-characterized materials certified for chemical composition or for some chemical or physical property. These materials are designated Standard Reference Materials® (SRMs) and are used to calibrate measuring instruments, to evaluate methods and systems, or to produce scientific data that can be referred readily to a common base. In this paper, we discuss the history of polymer based SRMs, their current status, and challenges and opportunities to develop new standards to address industrial measurement challenges.

Introduction

The main purpose of standard reference materials is to provide a well characterized material with a measured value and its associated uncertainty for some measurand such as a chemical concentration or some physical property. The SRMs in our portfolio focus on thermoplastic resins and address properties such as melt flow rate, molecular mass, molecular mass distribution, limiting viscosity, intrinsic viscosity, and heat capacity. Our portfolio is a good representation of the research focus of the Polymers Division in the 1970s with the emphasis on fundamental polymer analysis. These standards were sufficient for several decades as much of industrial advances were focused on synthetic efficiency, performance, and optimization of existing polymers and polymer additives and blends through improved processability and control of material properties. Concurrently, emerging technologies advancing polymerization processes and tailoring molecular mass and chain architecture were being promoted from fundamental research to more promising industrial applications. Thus, over time existing reference materials were no longer adequate to calibrate measurements of these new advanced materials. The challenge moving forward is to add novel materials to the NIST standards portfolio that are relevant to the modern plastics industry. Reference materials and measurements together must rise to the sophistication of modern polymers.

To address this challenge, we are updating our SRM portfolio (see Table 1) through a two-phase approach. First, current standards are being assessed for long term stability and continued needs. This assessment includes testing to ensure current standards meet the certified values and uncertainties listed in their certificates. As available, these certified values are also measured with the most recent measurement methods and protocols to retain relevancy to current measurement technologies. Inventory evaluation is also essential to determine if enough reference materials remain to fulfill demand. As the supply for a particular standards decreases, replacement material must be tested and certified. Review of existing SRMs indicate that some standards are being utilized for measurements beyond their certified values, or “off label” use. This knowledge not only allows NIST to focus our resources on supporting appropriate material standards, but can inform us about unmet needs and help direct our development of new reference materials. This goal will be achieved through stakeholder engagement to investigate where new reference materials will improve accuracy in measurements for manufacturing and what new materials are relevant and have a long term impact for polymer measurements and calibrations.

Two examples of NIST reference material evaluation and development are introduced for measurement of melt flow rates and molecular mass averages to highlight current progress and challenges in standards evaluation and development.

Melt Flow SRMs

The following example describes in general terms how we address updating the certificates for our melt flow SRMs. For the most part, ASTM-D-1238-XX with the XX referring to the year/version of the standard is the method followed to make the measurements. Thus, some SRMs used today may have been measured using a prior standard method. As noted in the Significance and Use section of the test method, it is primarily used for quality control purposes on thermoplastics as the flow rate value is not a fundamental polymer property and allows the user to assess the uniformity of the resin tested. [1] Our SRMs are used as a means of calibrating the instrument. To date, all of our SRMs use Procedure A in which resin is preheated for a set time, then a fixed load is used to help push the molten polymer through an orifice for a set period of time with the mass of the extrudate weighed and the melt index given in units of g/10 min. In general for this method, only the preheating time has changed, increasing from 6 min to 7 min. When stability testing or recertifying is conducted, it is important to remember to follow the method used when the material was certified. Once satisfied that the property has not changed, new

McDonough, Walter; Orski, Sara; Guttman, Charles; Migler, Kalman; Beers, Kathryn.
“Standard Reference Materials for the Polymers Industry.”
Paper presented at the Society of Plastics Engineers - Annual Technical Conference (SPE ANTEC), Indianapolis, IN, May 23-May 25, 2016.

values can be determined using the current standard method. For standard reference materials, not only is the mean and standard deviation calculated, but also the overall expanded uncertainty. For melt flow measurements, sources of uncertainty are due to:

- The repeatability of the experiment
- The instrument variability as estimated from precision tables in ASTM-D-1238
- Weighing
- Timing
- Temperature

The combined standard uncertainty is computed by root-sum-of-squares of the component uncertainties with the expanded uncertainty on the certificate being two times the combined standard uncertainty, which arises from a large number of degrees of freedom. [2] For the above sources of uncertainty, the dominant source comes from the instrument variability as estimated from precision tables in ASTM-D-1238. It was deemed to be reasonable to include this uncertainty as NIST uses a commercial instrument to conduct the experiments. The uncertainty due to temperature was the next largest source, with the remaining sources an order of magnitude less.

There has been interest expressed in having an SRM that can be used for Procedure B of ASTM D1238. This procedure is more automated than procedure A in that the flow rate is calculated from the machine measuring the volume of molten polymer pushed through the orifice over a set time. This value, combined with the density of the resin results in a melt flow rate value. Currently, the melt flow tables in ASTM D-1238 are being updated. Part of this effort includes testing materials using Procedure B. NIST could put forward one of the materials tested as a research or reference material while full scale testing is done to help the material eventually become a standard reference material. This includes a variety of molecular mass polymers and differing degrees of short and long chain branching.

Molecular Mass SRMs

Absolute techniques to measure number and mass average molecular masses, M_n and M_w, respectively, such as membrane osmometry and static light scattering, respectively, have been largely superseded by relative analytical methods such as size exclusion chromatography (SEC). SEC offers enhanced measurement precision even though material calibration standards are required to determine the molecular mass and molecular mass distribution. Standards development organizations have recognized this need and developed documentary standards for multi-detector SEC such as ISO 16014-(1 to 5) and ASTM D5296-11 to describe best practices for separation and analysis of polymers. ASTM has even assembled a task force to compare relative and absolute measurements to quantify bias, which is how well a test agrees with a generally accepted value. [3] NIST is adopting a similar approach to its molecular mass and molecular mass distribution SRMs, focusing on correlating the original certificate measurements and uncertainties with multi-detector SEC. NIST molecular mass SRMs consist of linear polyethylene, polystyrene, and poly(methyl methacrylate), which are no longer representative of the array of chemical and architectural control available to modern polymers.

A particular example is the evolution of polyolefins in industrial manufacturing. SRM 1475A, a broad distribution linear polyethylene (M_w = 52,000 g/mol) and standards derived from its fractions are widely used NIST standards for molecular mass and molecular mass distributions. These linear standards have been the hallmark of polyolefin calibration from NIST for the last 40 years. Advances in olefin methathesis using metallocene catalysts has vastly expanded the ability to control molecular mass and degree of long and short chain branching. Linear PE is not representative of the solution behavior of these materials and cannot alone be an adequate calibration standard for SEC. Novel infrared flow-through detection has expanded the ability to quantify average short chain branching at each point on a molecular mass distribution curve. Utilizing advanced metallocene catalysts, NIST is currently developing molecular mass and sequence controlled short chain branched polymers to be able to make reference materials that have quantified degree of alkyl branching (AB) and alkyl branching distributions (ABD). Furthermore, the majority of NIST standards certify either M_n or M_w, which represent only the first and second moments of the molecular mass distribution and are not fully descriptive of all molecular masses and associated error throughout the entire distribution curve. Analysis of these next-generation standards must address uncertainty in each slice of the distribution curve.

Challenges and Opportunities

Developing prototypes on new polymer standards is only the first step in creating new NIST standard reference materials. Production of a candidate material to a SRM can take three to five years from the laboratory to realization due to market research, scale-up, and exhaustive analysis to quantify all measurement uncertainties. NIST has recognized that for many fields, this time frame hinders emerging technology where non-equivalent standards are limiting further development and commercialization.

A proposed alternative is to expedite useful material to industry through the development of what are known as NIST Reference Materials (NIST RMs). These products would have “reference” rather than “certified” values and would not have all sources of uncertainty fully estimated, as required for a SRM. Thus these materials are provided with a report of investigation, not a certificate. Vetting of the material would be achieved by measurements from NIST as well as industrial partners willing to share analysis results on a collective database. The measurement values and uncertainties of a reference material may be sufficient for industrial needs or may be able to bridge the gap in time until NIST completes the full analysis and production of the material as an SRM.

Conclusions

Standard Reference Materials are used to calibrate measuring instruments, to evaluate methods and systems, or to produce scientific data that can be referred readily to a common base. As NIST updates and expands its polymer based reference material portfolio, it must maintain the high accuracy measurements of its current standard materials in their next generation materials. NIST strives to make the most precise and accurate measurements based on absolute methods. NIST must also recognize the utility of quantification at various levels of rigor to address immediate industrial needs, especially as absolute measurements for a specific material property are under development. This strategy will allow for the transition from standards expertise in classic thermoplastics to advanced materials relevant to commercial market today and well into the future.

References

1. ASTM D1238-13
2. ISO/IEC Guide 98-3:2008
3. ASTM D5296-11

Table 1: List of polymer SRMs with the associated properties measured

705a	Polystyrene (Narrow Molecular Weight Distribution)	Certified Value
706a	Polystyrene	M_w, Intrinsic Viscosity
1474a	Polyethylene Resin	Melt Flow Rate
1476a	Branched Polyethylene Resin	Melt Flow Rate
1478	Polystyrene (Narrow Molecular Weight Distribution)	M_w, M_n, Intrinsic Viscosity
1479	Polystyrene (Narrow Molecular Weight Distribution)	M_w
1484a	Linear Polyethylene (Narrow Molecular Weight Distribution)	M_w, M_n, Limiting Viscosity
1487	Poly (methyl methacrylate) 6 K Narrow Molecular Weight Distribution	M_w, Limiting Viscosity
1488	Poly (methyl methacrylate) 29 K Narrow Molecular Weight Distribution	M_n, Limiting Viscosity
1489	Poly (methyl methacrylate) 115 K Narrow Molecular Weight Distribution	M_n, Limiting Viscosity
1496	Unpigmented Polyethylene Gas Pipe Resin	Melt Flow Rate, Intrinsic Viscosity
2881	Polystyrene Absolute Molecular Mass Distribution Standard	Molecular Mass Distribution
RM 8281	Single-Wall Carbon Nanotubes (Dispersed, Length Resolved)	Ultra violet visible (UV-Vis) and UV-Vis-near infrared (NIR) absorbance spectra, Raman scattering ratio, NIR fluorescence, atomic force microscopy, transmission electron microscopy
1473b	Low Density Polyethylene Resin	Melt Flow Rate
1475a	Polyethylene, Linear	Melt Flow Rate, M_n, M_w, M_z, Limiting Viscosity, Solid Density, Heat Capacity
1482a	Polyethylene, 14 K Molecular Weight	M_w, M_n, Intrinsic Viscosity
1483a	Polyethylene, Linear	M_w, M_n, Intrinsic Viscosity

2885	Polyethylene (6280 g/mol)	M_w, Intrinsic Viscosity
2886	Polyethylene (87000 g/mol)	M_w, Intrinsic Viscosity
2887	Polyethylene (196,400 g/mol)	M_w, Intrinsic Viscosity

Minimizing Attack Graph Data Structures

Peter Mell
National Institute of Standards and Technology
Gaithersburg, MD United States
email:peter.mell@nist.gov

Richard Harang
U.S. Army Research Laboratory
Adelphi, MD United States
email:richard.e.harang.civ@mail.mil

***Abstract*— An attack graph is a data structure representing how an attacker can chain together multiple attacks to expand their influence within a network (often in an attempt to reach some set of goal states). Restricting attack graph size is vital for the execution of high degree polynomial analysis algorithms. However, we find that the most widely-cited and recently-used 'condition/exploit' attack graph representation has a worst-case quadratic node growth with respect to the number of hosts in the network when a linear representation will suffice. In 2002, a node linear representation in the form of a 'condition' approach was published but was not significantly used in subsequent research. In analyzing the condition approach, we find that (while node linear) it suffers from edge explosions: the creation of unnecessary complete bipartite sub-graphs. To address the weaknesses in both approaches, we provide a new hybrid 'condition/vulnerability' representation that regains linearity in the number of nodes and that removes unnecessary complete bipartite sub-graphs, mitigating the edge explosion problem. In our empirical study modeling an operational 5968-node network, our new representation had 94 % fewer nodes and 64 % fewer edges than the currently used condition/exploit approach.**

Keywords- attack graph; complexity analysis; data structures; minimization; representation; security.

I. Introduction

An attack graph is a representation of how an attacker can chain together multiple attacks to expand their influence within a network (often in an attempt to reach some set of goal states) [1]. Among other things, an attack graph can be used to calculate the threat exposure of critical assets, prioritize vulnerability remediation, optimize security investments, and as a tool to guide post-compromise forensic activities. Restricting attack graph size is vital for both human visualization of sub-graphs and the execution of high degree polynomial analysis algorithms. Early attack graph research used a 'state enumeration' representation [2] that would record all possible orderings by which an attacker could exploit a set of vulnerabilities, and hence grow at a factorial rate (exponential with some modifications). This rapid growth was mitigated in 2002 by a 'condition-oriented' approach providing a linear number of data objects with a quadratic worst-case number of relationships (with respect to the number of hosts in the original network) [3]. A major tenet of this approach was the assumption of 'monotonicity', which stated that an attacker would never lose a privilege once it was gained and any increase in privilege would not negate other gained privileges. This removed the need to account for the order in which attacks are initiated, and so reduced the complexity of the representation.

Subsequent research modified this model to make it attack- focused and enable humans to visually follow the steps within an attack more easily [2]. This hybrid 'condition/exploit' model [4] has been used extensively since 2003 for attack graph research. Unfortunately, we find that this model results in redundant data encodings, under which the worst-case graph size become quadratic in the number of nodes. Thus, over a decade of attack graph research has used a quadratic representation when a linear one was available in the literature.

However, even had the node linear condition-oriented approach been adopted, we find that it suffers from avoidable edge explosions (the creation of unnecessary complete bipartite sub-graphs) under certain conditions. These edge explosions add a quadratic factor to worst-case edge growth based on the maximum number of attacker privileges on any one host.

These size complexity issues are not always readily apparent from visual inspection of small example graphs. Example attack graphs in the literature to date have often contained a small number of dissimilar hosts with limited per-host attack surfaces and thus do not reveal the worst-case growth in both nodes and edges that we have observed. In large enterprise networks, however, where hosts have both large and diverse attack surfaces and are vulnerable to high-level compromise (thus yielding a high number of post-conditions), these complexity issues become much more evident.

To address these weaknesses, we provide a new hybrid 'condition/vulnerability' representation that regains linearity in the number of nodes and that does not suffer from the edge explosion problem. In our empirical study of a network model derived from an operational 5968-node network, our new representation had 94 % fewer nodes and 64 % fewer edges than the most widely cited recent approach in our surveyed literature (the condition/exploit model).

This reduced graph size will increase the speed of automated analysis, even making some algorithms tractable under certain scenarios. This can be true for higher polynomial complexity algorithms such as the cubic algorithms in [3] and certainly for metrics derived from attack graphs that grow either exponentially or with high polynomial degree [5]-[8] (as often occurs when graphs containing cycles must be rendered acyclic for the purposes of probabilistic modeling). The reduced size can also aid in human visualization and analysis of select sub-graphs of interest.

SP-639

Copyright (c) The Government of United States, 2015. Used by permission to IARIA. ISBN: 978-1-61208-438-1

The development of the work is as follows. In Section 2, we survey past attack graph representations and describe them in terms of four major categories (while citing minor variations). For each category, we provide a description, theoretical analysis of worst-case growth, and an example graph from previously published work. Section 3 then provides our two new representations that improve upon the worst-case node and edge growth of the other representations. Section 4 provides a theoretical analysis of set of analyzed approaches. Section 5 provides empirical results using a network model based on an operational network where we compare the attack graph sizes using the different approaches. Section 6 concludes the paper.

II. Survey of Attack Graph Representations

Papers discussing some abstraction of the attack graph idea began appearing as early as 1996 [9]-[12]. The first widely used representation was the ‘state enumeration’ approach ([2] and [13]-[16]) that had the unfortunate characteristic that it could grow faster than exponential. In 2002, the ‘condition-oriented’ approach was published with the express purpose of reducing the graph representation size down to polynomial complexity [3]. In 2003, the ‘exploit-oriented’ approach was published [17] to enhance the human readability of the graphs compared to the condition-oriented approach [2]. While not discussed in the literature, we will show that the exploit-oriented approach suffers high polynomial growth rates. This may explain why, in the same year, our surveyed literature moved to a more efficient hybrid ‘condition/exploit-oriented’ approach [4] (which we find still has a growth rate higher than that of the condition-oriented approach). Our literature survey shows that this approach has been used extensively since 2003 and is the predominant representation (e.g., [1], [4], [7], and [18]-[20]). The following subsections discuss each of these approaches in detail. It should be noted that each representation encapsulates the same underlying knowledge but using a different abstraction. For each type of representation, we analyze the worst-case growth rate of a resulting attack graph with respect to the number of nodes and edges. We define *h* to be the number of hosts in the associated physical network, *v* to be the maximum number of vulnerabilities on any one host, and *c* to be the maximum number of attacker privileges that can be achieved on any one host from the set of available vulnerabilities. For the graph size complexity analyses, we assume that there is a unique set of pre-conditions for each attack.

A. *State Enumeration*

State enumeration was the first widely used attack graph approach. Its distinguishing feature is that it explicitly accounts for the different orderings in which an attacker may launch attacks. There are two types. One type uses nodes to represent attacks and edges to represent post-conditions resulting in attacker privilege [13]-[15]. The other type uses nodes to represent attacker privilege and edges to represent attacks ([2] and [16]).

The graph design contains multiple layers of nodes, regardless of the particular node and edge semantics. The initially available set of conditions or attacks are presented at the top layer. Each subsequent lower layer represents the possible decisions that an attacker could make. Directed edges connect the nodes at one layer to the available nodes at the next lower layer. There are no edges between nodes at a particular layer. An attack scenario begins at the top layer and works its way down with the node chosen in each layer representing an attacker’s next decision.

1) Complexity Analysis

Assume that *v* and *c* equal 1. At the top layer (labelled 0), any of h hosts may be selected as the first node in the attack path. At layer 1, there are *h*-1 hosts that can be attacked from each of the h start nodes. For each node at layer 2 there are *h*-2 hosts that can be attacked, and so forth. This creates a rapidly expanding tree where the number of nodes and edges increases as O(*h*!), yielding a worst-case factorial growth rate for state enumeration graphs.

Most approaches attempt to prune this tree to focus only on subtrees of interest (e.g., those leading to some goal state). This can limit the growth, allow limited reuse of nodes, and can migrate the structure from a tree to a hierarchical directed graph with no loops (see Figure 1). Despite such optimizations, the growth rate of this approach is still worst-case exponential [2].

From an empirical perspective, such graphs become too large to be practical. For example, a network with just 5 hosts and 8 available exploits produced an attack graph with 5948 nodes and 68 364 edges [15].

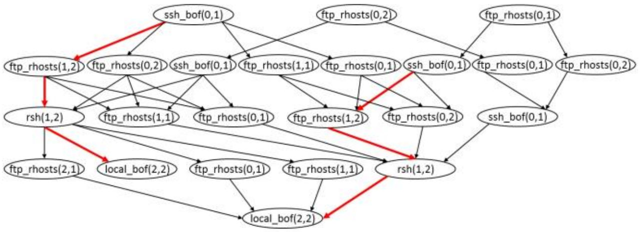


Figure 1. Example State Enumeration Attack Graph

Figure 1 shows an example pruned state enumeration attack graph, from [2], derived from an example with 2 target hosts running 2 services each, a single attacking host, and 4 unique attack types. Notice that the representation uses the previously discussed modifications to avoid factorial growth rate. The large red arrows highlight a remaining inefficiency by showing an example of path duplication in the graph (discussed in [2]).

Additional variations include [21]-[24].

B. *Condition-Oriented*

The condition-oriented approach was introduced in [3] as a method to reduce the representational complexity of the state enumeration approach by using the assumption of attacker privilege ‘monotonicity’. This assumption implies that an attacker never loses a privilege once it is gained, and any increased privilege will not negate any other privileges. In practice, it means that (unlike in the state enumeration approach) there is no longer any need to track the order in which attacks are initiated. This assumption has been found

SP-640

to be reasonable in most cases [2] and has been adopted by almost all subsequent attack graph representations.

The work of [2] introduced a graphical representation to the approach. Each ‘condition node’ represents some state of attacker privilege (e.g., execute as superuser on host x). An edge from node a to node b with label c represents that pre-condition a is necessary (but not necessarily sufficient) for attack c to provide privilege b. Sufficiency to gain privilege b is obtained if the pre-conditions of all edges into node b, labeled with c, are satisfied. By grouping the in-edges to each node by their edge labels, we can see that each group represents a possible attack, and each node is thus expressed in a variant of disjunctive normal form (DNF): in-edges within a group provide conjunctional logic and the distinct groups form logical disjunctions. Note that unlike general DNF statements, negation is not represented.

One limitation of the approach in [3] is that a single attack on a host that can be instantiated by different sets of pre-conditions must be represented by multiple attack instances named differently (using the edge names) to enable disjunctional logic. Distinct attack instances, involving different hosts, may be named similarly with no ambiguity.

1) *Complexity Analysis*

The condition-oriented approach achieves linearity in the number of nodes, significantly reducing the complexity compared to the state enumeration approach. An attacker may have up to c distinct condition states on each of the h hosts, and thus the number of nodes is bounded by hc. Unfortunately, as each of the hc condition nodes can be connected to all hc other nodes, and each connection between two nodes may have up to v edges to represent exploiting each available vulnerability, we obtain up to $hc\times hc\times v=h^2c^2v$ edges in the graph. Normally, h is much larger than c or v for a large network (as c and v are the maximums per node, not totals) and thus we can treat c and v as constants for the complexity analysis. Thus, the condition approach is O(h) in nodes and O(h^2) in edges, representing an enormous improvement over the exponential state enumeration approach. However, note the multiplicative c^2 term in the number of edges. This is the result of unnecessary complete bipartite sub-graphs forming under certain conditions. We analyze these edge explosion situations in more detail in Section 4.

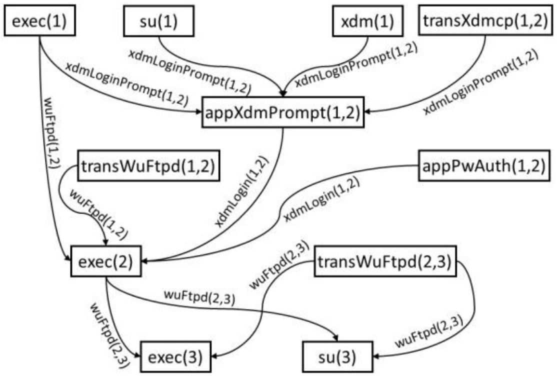


Figure 2. Example Condition-Oriented Attack Graph

Figure 2 shows an example condition-oriented attack graph, from [2], derived from a network with 2 target hosts, a single attacking host, and 3 unique attack types. Note the reduced complexity compared to Figure 1 although, as stated previously, these small example graphs are primarily intended to illustrate the methods, and do not demonstrate the differences in worst-case size complexities.

Additional variations include [21] and [25].

C. *Exploit-Oriented*

The exploit-oriented approach represents attacks as nodes and states of attacker privilege as edges ([2] and [17]) to ease visual analysis compared to the condition-oriented approach. Note that each ‘attack node’ is labeled with the host launching the attack and the host receiving the attack (which can be the same host for local attacks). This dual labeling on attack nodes will cause significant representational inefficiencies. The in-edges to a node represent the pre-conditions for launching an attack and the out-edges represent the post-conditions of the exploit. All out-edge post-conditions of a node are satisfied if and only if all the in-edge pre-conditions are satisfied.

Explicit representation of disjunction is not available and so in the presentation in the literature, attacks that can be instantiated by distinct sets of pre-conditions must be represented by multiple nodes. However, by applying a similar edge grouping approach as in the condition-oriented approach, this duplication of nodes can be avoided. Since the edges in this approach are already labeled with the post-condition names they must be additionally labeled with a grouping name (a name for the group of pre-conditions that will enable exercising the related exploit). While this modification is not discussed in the literature, we assume this optimization to represent the approach as efficiently as possible. Without this optimization, the number of nodes would increase by a factor of c.

1) *Complexity Analysis*

We now examine the worst-case growth rate of some arbitrary attack graph. With respect to nodes, the graph can grow as large as h^2v. Each of the h hosts can attack all h hosts with v different attacks (assuming just one attack per vulnerability) resulting in h^2v nodes. With respect to edges, the graph can grow as large as h^3v^2. Consider a single node where b represents the attack target. This node can have a connection to each node where the attack source is b. There will be hv nodes with attack source b. Each connection though can be made up of c edges. Thus, each node can create hvc out-edges. Since the number of nodes is h^2v, this leads us to $h^2v\times hvc=h^3v^2c$ edges. Treating c and v as constants compared to h, the exploit approach is O(h^2) in nodes and O(h^3) in edges. This is an enormous increase in graph size from the condition approach, however it still outperforms the exponential state enumeration approach.

Figure 3 shows an example exploit-oriented attack graph, from [2], derived from the same network as Figure 2. The example condition-oriented graph has 11 nodes and 12 edges while the example exploit-oriented graph as 6 nodes and 13 edges. Despite the reduction in graph size demonstrated in this example, we will empirically show that the exploit-oriented graphs can grow much larger than the condition-oriented graphs in enterprise networks.

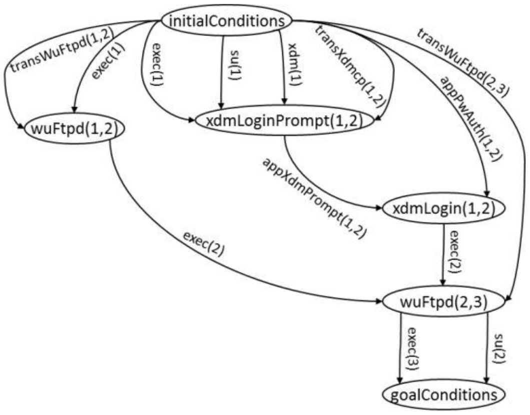


Figure 3. Example Exploit-Oriented Attach Graph

D. Hybrid Condition/Exploit-Oriented

The hybrid condition/exploit-oriented approach uses two distinct types of nodes ([1], [4], [7], and [18]-[20]) representing both attacks and the states of attacker privilege, while the edges are unlabeled. The ‘attack nodes’ and ‘condition nodes’ have the same semantics as those in the exploit-oriented graphs and the condition-oriented graphs, respectively.

This structure produces a directed bipartite graph, with attack nodes having edges to condition nodes and vice versa. However, the interpretation of the in-edges varies per type of node. Attack nodes and their post-condition out-edges are all satisfied if and only if all in-edges are satisfied (conjunction as with the exploit-oriented graphs). Condition nodes and their out-edges are satisfied if at least one in-edge is satisfied (disjunction as with multiple groups of in-edges in the condition-oriented graphs).

As in the exploit-oriented representation, the problem of a single exploit that can be instantiated with multiple sets of pre-conditions is not well addressed in the literature. In a naïve implementation, a single exploit must be divided into multiple attack node instances, one for each distinct set of pre-conditions. However, by applying the same optimization as before (again, not previously presented in the literature) where we allow condition node to attack node edges to be labeled with a group name, we can avoid this multiplication, and we assume this optimization throughout. As in the condition approach, the interpretation is disjunction among the groups and conjunction within a group. Without this optimization, the worst-case number of attack nodes would increase by a factor of c (as with the exploit approach).

1) Complexity Analysis

We now examine the worst-case growth rate of some arbitrary attack graph. With respect to nodes, the graph can grow as large as $hc+h^2v$. There will be hc condition nodes as derived in Section 2.2.1 and there will be h^2v attack nodes as derived in Section 2.3.1. With respect to edges, the condition and attack nodes form a directed bipartite graph. We first explore the set of attack to condition node edges. Each attack node has a single target host as discussed in Section 2.3. Each attack node then can at most activate c condition nodes on the target host where each activation creates an attack to condition node edge. Since there are up to h^2v attack nodes, we can then have up to $h^2v \times c = h^2vc$ attack node to condition node edges. Similarly, each condition node is mapped to a host, say a, and thus may have an edge to any of the hv exploit nodes where the attack source is a. Since there are hc condition nodes and up to hv edges per node, we get a total of $hc \times hv = h^2vc$ condition to exploit node edges. Summing the two types of edges, we get $h^2vc+h^2vc=2h^2vc$.

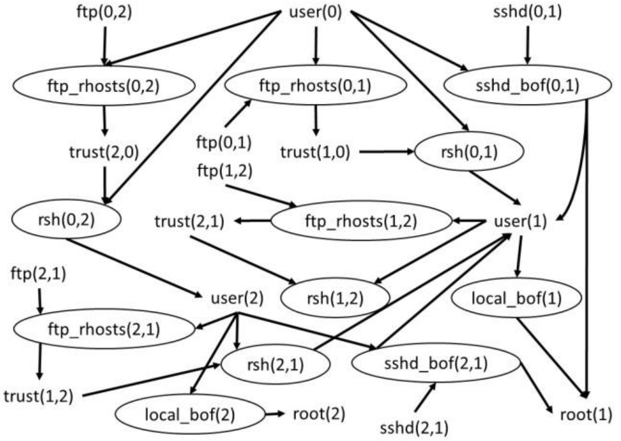


Figure 4. Example Condition/Exploit-Oriented Attack Graph

Figure 4 shows a condition/exploit-oriented attack graph from an example provided in [4]. This was derived from the same network as in Figure 1. The circled nodes are the attack nodes and the un-circled nodes are the condition nodes. Notice the relative simplicity in comparison with the state enumeration approach in Figure 1. Again though, the size of these small examples doesn’t demonstrate complexity growth on large enterprise networks.

Additional variants include [26]-[28].

III. VULNERABILITY-BASED REPRESENTATIONS

Our contribution is the idea of representing the vulnerabilities on specific hosts explicitly within attack graphs. From a visualization point of view, this makes it easy to see how a chain of vulnerabilities (and hosts) can be compromised. From a graph complexity point of view, the vulnerability nodes replace the use of the attack nodes thereby lowering node complexity to linear (from quadratic). Intuitively, where exploit nodes must contain references to both the source and target hosts in an attack step, and thus grow potentially quadratically in highly connected networks, the vulnerability nodes only reference the exploitable host, and so grow only linearly. We represent attacks within the edges where they can take advantage of the fact that edges inherently have sources and targets (similar to the condition approach).

This approach leads to two new representations that build upon one another. We first describe a vulnerability-oriented approach where we replace the attack nodes from the exploit-oriented approach with vulnerability nodes. This reduces node complexity from quadratic to linear and edge

SP-642

Copyright (c) The Government of United States, 2015. Used by permission to IARIA. ISBN: 978-1-61208-438-1

complexity from cubic to quadratic. We then point out how the vulnerability-oriented approach suffers from similar quadratic edge explosion scenarios as the condition approach (but this time relative to *v*, not *c*).

We then build upon the vulnerability approach to provide a hybrid condition/vulnerability representation that has a linear number of nodes, quadratic number of edges, and that does not suffer from quadratic edge explosion (in either *v* or *c*). It also, like the hybrid condition/exploit approach, improves on the human readability of the condition-oriented approach.

A. Vulnerability-Oriented

Our first approach is analogous to the exploit-oriented approach except that we replace the attack nodes with vulnerability nodes. A vulnerability node is labeled with a vulnerability name and the relevant location in the network (usually but not necessarily a hostname). Edges represent attacker privilege, just like in the exploit-oriented approach. In cases where multiple sets of pre-conditions can activate a particular vulnerability, we handle it with the edge grouping optimization we've presented previously. A set of pre-conditions that will activate a vulnerability are represented by a set of in-edges to a node that all have a common group name. Thus we represent attacks using groups of commonly named edges just like in the condition approach. Each node is thus expressed in DNF: in-edges within a group provide conjunctional logic and the distinct groups form logical disjunctions.

1) Complexity Analysis

We now examine the worst-case growth rate of some arbitrary attack graph. With respect to nodes, the graph can grow as large as *hv* because each of the *h* hosts can have *v* vulnerabilities. With respect to edges, each node can have *hv* outgoing connections to other nodes. Each connection can be made up of at most *c* edges. Thus, the total number of edges is at most $hv \times hv \times c = h^2v^2c$.

A disadvantage of this approach is the v^2 term in the number of edges. This is the result of unnecessary complete bi-partite sub-graphs forming under certain conditions. We analyze this edge explosion in more detail in Section 4.

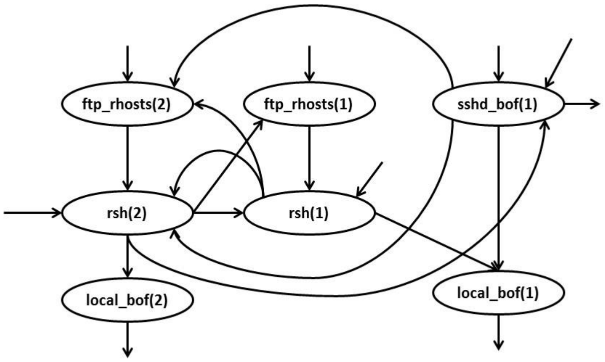


Figure 5. Example Vulnerability-Oriented Attack Graph

Figure 5 shows an example of a vulnerability-oriented graph, derived from the representation in Figure 4. For the sake of readability, edge grouping labels are omitted. Note that the number of nodes is reduced with respect to Figure 4, and all vulnerabilities are in exactly one node instead of replicated over multiple nodes with different attack sources (e.g., the attacks targeting the ftp rhosts vulnerability on node 1 in Figure 4).

B. Hybrid Condition/Vulnerability-Oriented

Our second novel approach is a hybrid approach combining condition nodes with our new vulnerability nodes. The condition nodes are analogous to those in the condition-oriented approach. The vulnerability nodes are identical to those in our vulnerability-oriented representation. We represent attacks by labeling the condition node to vulnerability node edges with the attack instances being used (including source and destination hostnames/IPs where applicable); this edge labeling is similar to that in the condition-oriented graphs. We then connect the vulnerability nodes to the condition nodes with unlabeled edges showing which post-conditions emerge as a result of exploiting the relevant vulnerability instance.

As with the hybrid condition/exploit graph, this structure produces a directed bipartite graph. For condition nodes, they and all of their attack labeled out-edges are satisfied if at least one in-edge is satisfied (disjunction). For vulnerability nodes, they and all of their unlabeled out-edges are satisfied if and only if a group of identically labeled in-edges are satisfied (conjunction within a group and disjunction between the groups). This distributed implementation of disjunctions and conjunctions enables the same DNF logic of the condition-oriented approach.

A single attack that can be instantiated with multiple sets of pre-conditions can be represented by using a different group name for each set of instantiating pre-conditions.

1) Complexity Analysis

We now examine the worst-case growth rate of an arbitrary attack graph. With respect to nodes, the graph can grow as large as $h(c+v)$. There will be *hc* condition nodes as derived in Section 2.2.1 and *hv* vulnerability nodes as derived Section 3.1.1. Thus, there are at most *hc*+*hv* nodes total. With respect to edges, there can be as many as $h^2cv+hvc$. First, for the set of edges that point from vulnerability nodes to condition nodes, each of the *hv* vulnerability nodes can activate up to *c* condition nodes (since each vulnerability pertains to a host with up to *c* conditions), creating *hvc* edges. In the other direction, each of the *hc* condition nodes could allow an attack to all *hv* vulnerability nodes, producing *hc***hv* edges. Thus, the total number of edges is $hvc+hc*hv=h^2cv+hvc$.

Treating *c* and *v* as constants compared to *h*, the condition/vulnerability approach is O(*h*) in nodes and O(h^2) in edges. This is a major improvement over the quadratic growth in the number of nodes caused by attack nodes in the exploit and condition/exploit approaches. While the complexity of the number of nodes is of the same order between the condition, vulnerability, and condition/vulnerability graphs, we note that there is no *v*2 or c^2 term in the edge growth equation for the condition/vulnerability graph. This is indicative of the fact that this approach does not suffer from the quadratic edge

SP-643

Copyright (c) The Government of United States, 2015. Used by permission to IARIA. ISBN: 978-1-61208-438-1

explosion problem of the condition and the vulnerability-oriented approaches in either *v* or *c*. This is discussed in detail in Section 4.

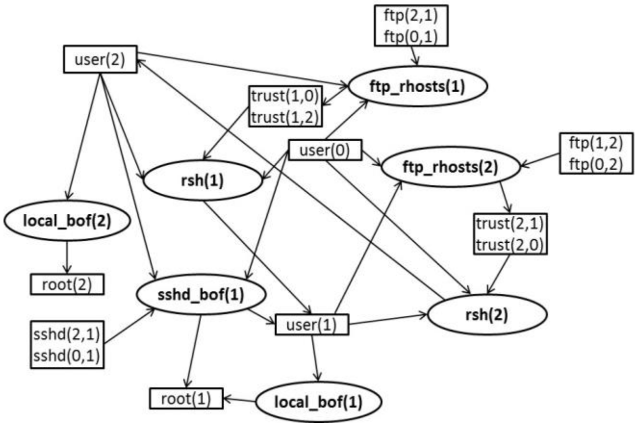


Figure 6. Example Condition/Vulnerability-Oriented Attack Graph

Figure 6 shows an example of the condition/vulnerability graph displaying the same attack graph data as in Figure 4 and Figure 5. In this example with just 3 nodes and relatively diverse attack surfaces, this data actually has a more compact representation in the vulnerability graph format. We demonstrate in Section 5 on larger scale real-world data that this advantage is not general, and in fact the condition/vulnerability graph provides significant size advantages in such cases.

IV. Theoretical Analysis

In this section, we provide a theoretical analysis of the worst-case behavior of the representations. Note that we do not analyze the state enumeration approach given its known exponential growth rate (previously discussed). We begin with a review of the big-O complexity of each graph type and show the advantages of the condition, vulnerability, and condition/vulnerability approaches. We then follow with an analysis of the terms within the actual worst-case growth equations. These equations reveal quadratic terms in both *v* and *c* that cause the edge explosion scenarios in the condition and vulnerability approaches, respectively. We then explore in more detail when and why these avoidable edge explosion scenarios occur. We end the section with a discussion of edge explosion scenarios that are unavoidable in all of our analyzed representations (and that may reflect an inherent limit in reducing graph sizes).

A. Big-O Complexity Graph Growth Comparisons

In an attack graph, *h* is expected to grow much larger than *v* or *c* for a typical enterprise network. Note that *v* and *c* are the maximums per host (not the total number of vulnerability and conditions) and thus are usually miniscule compared to *h*. For this reason, we treat *v* and *c* as constants to derive overall complexity of each representation. These big-O measurements were derived in Sections 2 and 3 and are summarized in Table 1. The calculations showing the largest growth rates are bolded. Note, if *h* is not large relative to *v* or *c*, use the below Table 2 instead of Table 1 to determine the most efficient representation.

Table 1. Complexity Measurement of Attack Graph Representation

Representation	Nodes	Edges
Condition	$O(h)$	$O(h^2)$
Exploit	$\mathbf{O(h^2)}$	$\mathbf{O(h^3)}$
Vulnerability	$O(h)$	$O(h^2)$
Condition/Exploit	$\mathbf{O(h^2)}$	$O(h^2)$
Condition/Vulnerability	$O(h)$	$O(h^2)$

The quadratic node growth of the exploit and condition/exploit approaches is much larger than the linear node growth of the condition and condition/vulnerability approaches. With respect to edges, the cubic edge growth of the exploit approach is larger than the quadratic growth of the other approaches. Thus, the condition, vulnerability, and condition/vulnerability approaches are the best approaches in limiting worst-case graph growth with respect to *h*.

To intuitively understand why the exploit and condition/exploit node growth is quadratic, consider that an exploit node must necessarily contain two host name labels: the attack source and the attack target. If a set of hosts A can attack a set of hosts B using a single attack, then the number of exploit nodes representing this will be |A|*|B| (i.e., quadratic growth). Contrast this to the condition/vulnerability approach where there will be only a single vulnerability node per host in B resulting in |B| vulnerability nodes (i.e., linear growth).

One optimization is to reduce graph size by consolidating groups of identical hosts (those with identical security value, vulnerabilities, and permitted connectivity) into single hosts when building the attack graph. This essentially reduces *h* and thus minimizes the graph size, but we note that it does not change the big-O complexity results nor the outcome of our comparative analyses.

B. Worst-Case Equations Graph Growth Comparisons

We now look at the actual worst-case equations that we derived in Sections 2 and 3 in order to further refine our comparison between the approaches. These equations are summarized in Table 2. The terms specifically discussed in our analysis are bolded.

Table 2. Worst-Case Growth of Attack Graph Representations

Representation	Nodes	Edges
Condition	hc	$h^2v\mathbf{c^2}$
Exploit	h^2v	h^3v^2c
Vulnerability	hv	$h^2\mathbf{v^2}c$
Condition/Exploit	$hc+h^2v$	$2h^2vc$
Condition/Vulnerability	$\mathbf{hc+hv}$	$h^2\mathbf{vc}+hvc$

We focus our analysis on the condition, vulnerability, and condition/vulnerability approaches since the other two approaches were shown to have larger big-O node complexities in Table 1.

With respect to node growth, the condition and vulnerability approaches will always have fewer nodes than the condition/vulnerability approach due it having the sum of

Copyright (c) The Government of United States, 2015. Used by permission to IARIA. ISBN: 978-1-61208-438-1

the former two. However, it should be noted that this increase is a small linear factor.

With respect to edge growth, however, both the condition and vulnerability graphs grow quadratically in *c* and *v*, respectively. It is these quadratic terms (not present in the condition/vulnerability edge equation) that reflect edge explosion scenarios where unnecessary complete bipartite sub-graphs are formed. We claim that they are unnecessary because the condition/vulnerability approach provides a linear representation of the same data. Visually, the condition and vulnerability approaches use complete bi-partite sub-graphs where, for the same data, the condition/vulnerability approach uses star topologies (explained in detail in the next section).

Thus overall, our theoretical analysis indicates that our condition/vulnerability approach will result in achieving the most compact attack graphs. The exploit approach was the worst (excluding the naïve state enumeration approach), suffering from cubic edge growth. The condition/exploit approach (the most commonly used in recent research in our surveyed literature) suffered from quadratic node growth in our largest term, *h*. Finally, the condition and vulnerability approaches suffered from quadratic edge explosions (in *c* and *v*, respectively) as a result of the creation of complete bi-partite sub-graphs that our condition/vulnerability approach converts to linear growth star topologies. We now explore in detail the edge explosion scenarios.

C. *Avoidable Edge Explosion Scenarios*

We define an edge explosion as the creation of a complete bipartite sub-graph within an attack graph due to some specific scenario. Some scenarios cause edge explosions regardless of which of our analyzed attack graph representations is used. We call these scenarios ‘unavoidable’ (with respect to our set of representations) and thus they are not useful for a comparative analysis. We discuss such unavoidable scenarios in the next section.

This section focuses on avoidable scenarios that create quadratic edge explosions in the condition and vulnerability representations, which are converted to linear star representations in the condition/vulnerability approach. The condition/exploit approach has similar representational advantages with respect to edge explosion scenarios. However, we do not specifically analyze this for the condition/exploit approach due to its worse quadratic node complexity but we do note that it is the dual node type representations that enable the reduction (i.e., the ‘hybrid’ node design).

Avoidable edge explosion can occur in both the condition and vulnerability graphs as shown by their worst-case quadratic growth in *c* and *v*, respectively. These upper bounds are approached in condition graphs whenever a single attack has multiple pre-conditions and multiple post-conditions. This also happens in vulnerability graphs when some set of vulnerabilities on a host allows subsequent exploitation of some other set of vulnerabilities (on the same or other hosts).

Both cases can be viewed in terms of directed hyperedges, representing the multi-way relationships. For example, an attack with multiple pre-conditions and post-conditions can be represented by a single directed hyperedge with the pre-conditions at the tail of the edge and the post-conditions at the head. In standard directed graphs, representing this requires the creation of a complete directed bipartite sub-graph with the pre-conditions in the edge ‘tail’ set and the post-conditions in the ‘head’ set. The representation of these hyperedges by the corresponding complete bipartite graphs is then responsible for the quadratic explosion in the number of edges. Similarly, given a set of vulnerabilities on a host where each one enables an attacker to exploit some other common set of vulnerabilities can be represented by a single directed hyperedge. In a vulnerability graph, this hyperedge would require a directed complete bipartite graph with the enabling vulnerabilities in the edge ‘tail’ set and the newly available vulnerability nodes in the edge ‘head’ set.

Hybrid node graphs, such as the condition/vulnerability and the condition/exploit graphs, represent these directed hyperedges more efficiently (i.e., linearly). To see this, consider that in the condition/vulnerability graph, each vulnerability node may represent a directed hyperedge that links multiple pre-conditions to multiple post-conditions. Each condition node may also represent a directed hyperedge that links multiple vulnerabilities on a single host to a set of common target vulnerabilities. This representational approach of a directed hyperedge forms a star graph for each hyperedge. It is then easy to see that star graphs grow linearly in the number of edges while the complete bipartite sub-graphs grow quadratically, thus enabling the size complexity advantage of the hybrid node approaches.

For the purposes of illustration, consider Figure 7 below. Conditions C_1 to C_4 form the tail of a hyperedge corresponding to a vulnerability V_a, while conditions C_5 to C_8 for the head. The resulting condition graph is complete bipartite, as each of C_1 to C_4 must be linked to each of C_5 to C_6 (Figure 7, left); by contrast, using a separate class of node to represent the vulnerability-related hyperedge in the condition/vulnerability approach allows for a much more compact representation in the form of a star graph (Figure 7, right).

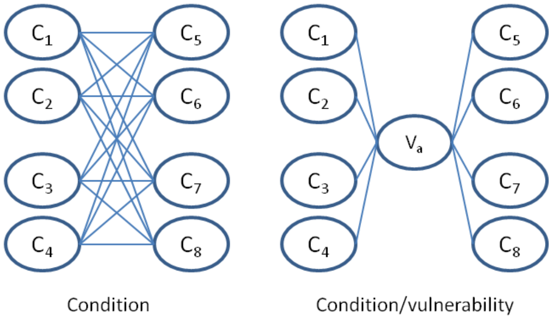


Figure 7. Unnecessary complete bipartite structures in the condition-oriented graph

Vulnerability graphs have a directly analogous representation, where a condition node may represent a hyperedge, as shown in Figure 8.

Copyright (c) The Government of United States, 2015. Used by permission to IARIA. ISBN: 978-1-61208-438-1

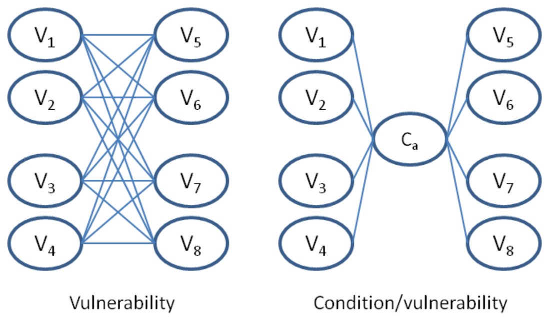


Figure 8. Unnecessary complete bipartite structures in the vulnerability-oriented approach

In the vulnerability graph, each vulnerability (V_1 to V_4) on a single host must have an edge to each vulnerability that is now accessible for attack (V_5 to V_8). In the condition/vulnerability graph, a single condition node C_a represents the attacker privileges gained by exploiting V_1 to V_4. Condition node C_a then allows exploitation of V_5 to V_8. The addition of C_a creates a linear growth star graph in place of the quadratic complete bipartite graph in the vulnerability representation.

D. *Unavoidable Edge Explosion Scenarios*

There are cases where the condition/vulnerability graph will still contain complete bipartite components and it is direct to see that the related condition or vulnerability graph will also exhibit such a component. Thus, such scenarios are unavoidable (with our set of analyzed representations). While we can't prove nonexistence of a linear representation here, we believe it unlikely and that we are pushing against inviolable data representational boundaries in trying to further reduce the size of the attack graph.

Consider a scenario where multiple distinct hyperedges have identical head or tail sets in either the condition- or vulnerability- oriented approach. This will naturally result in complete bipartite components in the condition/vulnerability representation; however, it is straightforward to see that such cases also produce complete bipartite graphs in the condition and vulnerability representations as well.

See, for example, the condition/vulnerability graphs in Figure 9. The leftmost panel depicts a situation in which two distinct vulnerabilities have identical head and tail sets (such as two identical vulnerabilities on two different hosts that each enable a common set of vulnerabilities on a third); the center depicts a situation in which the head sets are distinct but the tail sets are identical (perhaps granting host-specific post-conditions), and the rightmost pane depicts identical head sets with distinct tail sets (such as would be expected from host-specific pre-conditions with global post-conditions). In each case, it is straightforward to see that a path exists from each pre-condition to each post-condition, and so the resulting condition-oriented graph will be a complete bi-partite graph.

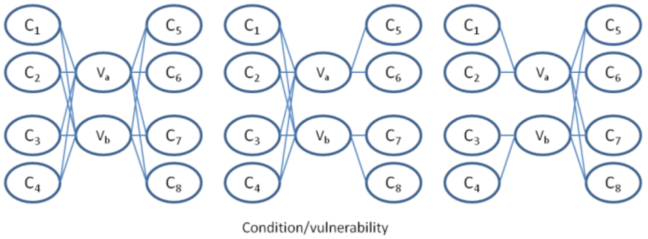


Figure 9. Condition/Vulnerability Graph Scenarios

The situation is functionally identical for vulnerability-oriented graphs. Similar complete bipartite sub-graphs within a condition/vulnerability graph will result in a completely connected bipartite sub-graphs in the related vulnerability graph.

Looking at the underlying equations, note that in the condition/vulnerability graph the number of edges is bounded as the product of c and hv, rather than being quadratic in c, thus requiring both v and c to grow simultaneously for a comparable edge explosion. Note that this doesn't reflect a unique weakness for the condition/vulnerability approach as both the condition and vulnerability approaches also contain h, c, and v in their edge equations (but there with a quadratic c or v). This worst-case scenario is only realized in the leftmost panel of Figure 9, while all three panels result in complete bipartite sub-graphs in the case of the condition-oriented graph.

V. Empirical Results

We now provide an example to illustrate the performance between the different approaches using a network model. Our network model (derived in part from data from an operational network) has 5968 hosts and 7825 vulnerabilities. The vulnerabilities consist of 41 distinct types mapped to two different severity levels. We mapped 7791 vulnerability instances to confidentiality breaches and 34 instances to providing user level access.

With respect to attack post-conditions, a vulnerability was modeled as producing two post-conditions: the severity level mapped to the host name and a designator indicating that the host had some specific vulnerability exploited. This models the situation where a single attack can produce multiple post-conditions.

With respect to connectivity, we modeled all nodes as being logically connected to each other. For a start node in the attack graph, we designated one of the hosts as hostile (using one with no vulnerabilities) to represent an insider threat situation.

Table 3 provides the empirical results given the above stated scenario. To derive these results, we created an attack graph simulator using Python 2.7.6 that calculates the graph sizes using all of our analyzed representations. Note that these results are not based on the equations from Table 2 as those equations represent worst-case attack graph sizes. Here we analyze the actual sizes given the network model described above.

SP-646

Copyright (c) The Government of United States, 2015. Used by permission to IARIA.

ISBN: 978-1-61208-438-1

TABLE 3. EMPIRICAL RESULTS

Graph Type	Nodes	Edges
Condition	5140	436 290
Exploit	218 146	7 189 929
Vulnerability	7825	272 920
Condition/Exploit	223 285	654 435
Condition/Vuln.	12 964	233 795

As expected from the theoretical analysis, the number of nodes for the exploit and condition/exploit representations was much larger than the other approaches due to the O(h^2) growth rate. The number of edges in the condition graph is almost twice that of the condition/vulnerability graph, attributable to the O(c^2) growth rate of the edges. Thus based on these empirical results, the vulnerability and condition/vulnerability approaches appear the best for our scenario and are comparable (with the vulnerability approach having fewer nodes and the condition/vulnerability approach having fewer edges).

Note how in this example our condition/vulnerability approach had 94 % fewer nodes and 64 % fewer edges than the widely cited and commonly used condition/exploit approach. This illustrates how an adjustment in representation can have dramatic results in graph size.

However, if we model each attack as producing exactly one post condition, then the advantages of the condition/vulnerability approach disappear relative to the condition graph (see Table 4).

TABLE 4. SINGLE POST CONDITION EMPIRICAL RESULTS

Graph Type	Nodes	Edges
Condition	2584	218 145
Exploit	218 146	7 189 929
Vulnerability	7825	272 920
Condition/Exploit	220 728	436 290
Condition/Vuln.	10 408	225 970

Here the condition graph has an advantage on the number of nodes while roughly matching the number of edges of the conditional/vulnerability approach. Thus, use of the vulnerability/condition approach does not guarantee a smaller graph than the condition representation. However, it guarantees a linear growth rate with respect to *c*, allowing for tighter representations given arbitrary scenarios.

Note that the vulnerability approach statistics stay the same in both Table 3 and Table 4. This is because the removed post conditions were not ones that enabled an attack to be launched (we just removed the flag that a host had a specific vulnerability exploited).

The widely-cited and used condition/exploit model was much larger in all of our scenarios because it suffers from both the O(h^2) growth rate in the nodes (this is true also of the exploit approach). Had we modeled a network where the logical connectivity of the hosts was much more restricted, the node disadvantage of the condition/exploit approach would have been minimized. However, many operational networks (including this one) have large numbers of hosts with significant logical connectivity (e.g., approaching complete sub-graphs).

VI. CONCLUSIONS

For the last decade, the condition/exploit-oriented approach was the most commonly used representation in our literature survey. However, we found it to have node growth quadratic in the number of hosts on the network. This will slow down analysis algorithms that have a high polynomial degree while making visualization for humans more difficult (simply from the increased size). Interestingly, we found the previously published condition approach provided a much more compact linear node representation, but it wasn't widely adopted. This may have been because it was confusing to visually analyze since attacks are represented by collections of edges. We also discovered that it suffers from quadratic edge explosions based on the number of possible attacker privileges on a host.

To address these problems, we proposed using a vulnerability-based approach for nodes in attack graphs. This eliminates the inefficiency of the attack nodes (taking us from a quadratic to a linear node representation) while it makes the graph more intuitive to read compared to the condition approach (since any attack results in compromising a single vulnerability node as opposed to activating multiple condition nodes). Surprisingly, we found this approach to also contain an edge explosion problem but this time relative to the number of vulnerabilities on a host.

We thus developed the hybrid condition/vulnerability approach with the following advantages: linear node growth, elimination of avoidable edge explosion issues, and an easy to understand representation (due to the use of the vulnerability nodes). For arbitrary graphs, our condition/vulnerability approach provides better size guarantees with respect to edge growth while only having a small linear penalty on node growth.

Despite this, the condition and vulnerability approaches are still viable representation options (linear in node growth and quadratic in edge growth). Even with the quadratic edge explosion possibilities, they can be used when it is known that a particular scenario will not suffer significantly from this problem. Perhaps the best argument for using these two approaches is simply that they have a single interpretation for the nodes. This should facilitate the application of standard graph algorithms for analysis, something not available with the currently used hybrid condition/exploit approach or our hybrid condition/vulnerability approach. Given the simple interpretation of our vulnerability approach, it is a candidate for exploration in this area, which may be addressed in future work.

Lastly and most importantly, we emphasize that the research community should move away from using attack nodes (as found in both the exploit representation and the hybrid condition/exploit representation) since the attack nodes add a quadratic factor to the worst-case node growth equations. Moving to a much more compact node linear representation (regardless of the specific choice) may catalyze the research community by opening the door to previously intractable algorithmic analyses and facilitating human analysis of specific features.

REFERENCES

[1] A. Singhal and X. Ou, "Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs," National Institute of Standards and Technology Interagency Report 7788, 2011.

[2] S. Noel and S. Jajodia, "Managing Attack Graph Complexity Through Visual Hierarchical Aggregation," in Workshop on Visualization and Data Mining for Computer Security, Fairfax, 2004, pp. 109-118.

[3] P. Ammann, D. Wijesekera and S. Kaushik, "Scalable, Graph-Based Network Vulnerability Analysis," in ACM Conference on Computer and Communications Security, Washington, D.C., 2002, pp. 217-224.

[4] S. Noel, S. Jajodia, B. O'Berry and M. Jacobs, "Efficient Minimum-Cost Network Hardening Via Exploit Dependency Graphs," in Computer Security Applications Conference, Las Vegas, 2003, pp. 86-95.

[5] M. Frigault, L. Wang, A. Singhal and S. Jajodia, "Measuring Network Security Using Dynamic Bayesian Network," in Proceedings of the 4th ACM Workshop on Quality of Protection, 2008, pp. 23-30.

[6] L. Wang, T. Islam, T. Long, A. Singhal and S. Jajodia., "An Attack Graph-Based Probabalistic Security Metric," in Data and Applications Security XXII, Springer, 2008, pp. 283-296.

[7] N. Idika and B. Bhargava, "Extending Attack Graph-Based Security Metrics and Aggregating Their Application," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 1, 2012, pp. 75-85.

[8] J. Homer, X. Ou and D. Schmidt, "A Sound and Practical Approach to Quantifying Security Risk in Enterprise Networks," Kansas State University Technical Report, 2009.

[9] M. Dacier, Y. Deswarte and M. Kaaniche, "Quantitative Assessment of Operational Security: Models and Tools," LAAS Research Report 96493, 1996.

[10] I. Moskowitz and M. Kang, "An Insecurity Flow Model," in New Security Paradigms Workshop, 1997, pp. 61-74.

[11] C. Meadows, "A Respresentation of Protocol Attacks for Risk Assessment," Network Threats, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 38, 1998, pp. 1-10.

[12] C. Phillips and L. Swiler, "A Graph-Based System for Network-Vulnerability Analysis," in Proceedings of the 1998 Workshop on New Security Paradigms, Charlottesville, 1998, pp. 71-79.

[13] R. Ortalo, Y. Deswarte and M. Kaaniche, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security," IEEE Transactions on Software Engineering, vol. 25, no. 5, 1999, pp. 633-650.

[14] L. Swiler, C. Phillips, D. Ellis and S. Chakerian, "Computer-Attack Graph Generation Tool," in DARPA Information Survivability Conference, Anaheim, 2001, pp. 307-321.

[15] O. Sheyner, J. Haines, S. Jha, R. Lippman and J. Wing, "Automated Generation and Analysis of Attack Graphs," in IEEE Symposium on Security and Privacy, Washington D.C., 2002, pp. 273-284.

[16] S. Jha, O. Sheyner and J. Wing, "Two Formal Analyses of Attack Graphs," in IEEE Computer Security Foundations Workshop, Cape Breton, 2002, pp. 49-63.

[17] S. Jajodia, S. Noel and B. O'Berry, "Topological Analysis of Network Attack Vulnerability," in Managing Cyber Threats: Issues, Approaches and Challenges, Kluwer Academic Publisher, 2003, pp. 247-266.

[18] S. Noel and S. Jajodia, "Measuring Security Risk of Networks Using Attack Graphs," International Journal of Next-Generation Computing, vol. 1, no. 1, 2010, pp. 135-147.

[19] J. Pamula, P. Ammann, S. Jajodia and V. Swarup, "A Weakest-Adversary Security Metric for Network Configuration Security Analysis," in Workshop on Quality of Protection, Alexandria, 2006, pp. 31-38.

[20] L. Wang, S. Noel and S. Jajodia, "Minimum-Cost Network Hardening Using Attack Graphs," Computer Communications, 2006, pp. 3812-3824.

[21] B. Schneier, "Attack trees," Dr. Dobb’s journal, 1999, pp. 21-29.

[22] B. Kordy, S. Mauw, S. Radomirović and P. Schweitzer, "Foundations of attack–defense trees," in Formal Aspects of Security and Trust, Springer , 2011, pp. 80-95.

[23] V. Gorodetski and I. Kotenko, "Attacks against computer network: Formal grammar-based framework and simulation tool," in Recent Advances in Intrusion Detection, 2002, pp. 219-238.

[24] R. W. Ritchey and P. Ammann, "Using model checking to analyze network vulnerabilities," in 2000 IEEE Symposium on Security and Privacy, 2000, pp. 156-165.

[25] J. Dawkins and J. Hale, "A systematic approach to multi-stage network attack analysis," in Proceedings, Second IEEE International Information Assurance Workshop, 2004, pp. 48-56.

[26] N. Poolsappasit, R. Dewri and I. Ray, "Dynamic security risk management using bayesian attack graphs," IEEE Transactions on Dependable and Secure Computing, 2012, pp. 61-74.

[27] D. Koller and N. Friedman, Probabilistic graphical models: principles and techniques, MIT Press, 2009.

[28] S. J. Templeton and K. Levitt, "A requires/provides model for computer attacks," in Proceedings of the 2000 Workshop on New Security Paradigms, 2001, pp. 31-38.

[29] R. Lippmann, K. Ingols, C. Scott and K. Piwowarski, "Validating and Restoring Defense in Depth Using Attack Graphs," in Military Communications Conference, Washington, D.C., 2006, pp. 1-10.

[30] S. Nanda and N. Deo, "A Highly Scalable Model for Network Attack Identification and Path Prediction," in SoutheastCon, Richmond, 2007, pp. 663-668.

Copyright (c) The Government of United States, 2015. Used by permission to IARIA. ISBN: 978-1-61208-438-1

Proceedings of ASME 2016 International Manufacturing Science and Engineering Conference
MSEC 2016
June 27 – July 1, 2016, Blacksburg, VA, USA

MSEC2016-8629

AUTOMATING ASSET KNOWLEDGE WITH MTCONNECT

Sid Venkatesh, Sidney Ly and Martin Manning
Boeing Company
Seattle, WA

John Michaloski and Fred Proctor
National Institute of Standards
and Technology
Gaithersburg, Maryland, USA

ABSTRACT

In order to maximize assets, manufacturers should use real-time knowledge garnered from ongoing and continuous collection and evaluation of factory-floor machine status data. In discrete parts manufacturing, factory machine monitoring has been difficult, due primarily to closed, proprietary automation equipment that make integration difficult. Recently, there has been a push in applying the data acquisition concepts of MTConnect to the real-time acquisition of machine status data. MTConnect is an open, free specification aimed at overcoming the "Islands of Automation" dilemma on the shop floor. With automated asset analysis, manufacturers can improve production to become lean, efficient, and effective. The focus of this paper will be on the deployment of MTConnect to collect real-time machine status to automate asset management. In addition, we will leverage the ISO 22400 standard, which defines an asset and quantifies asset performance metrics. In conjunction with these goals, the deployment of MTConnect in a large aerospace manufacturing facility will be studied with emphasis on asset management and understanding the impact of machine Overall Equipment Effectiveness (OEE) on manufacturing.

Keywords

MTConnect, asset management, Overall Equipment Effectiveness (OEE), manufacturing, Computerized Numerical Control (CNC), network

Nomenclature

AGFM	American Gesellschaft fr Fertigungstechnik und Maschinenbau
AGV	Automated Guided Vehicle
API	Application Programming Interface
CMM	Coordinate Measuring Machine
CNC	Computer Numerical Control
CTLM	Contour Tape Laying Machines
DCOM	Distributed Component Object Model
DST	Dörries Scharmann Technologie
EDM	Electro Discharge Machining
Focas	Fanuc OpenFactory CNC API Specifications
HSSB	High Speed Serial Bus
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
KPI	Key Performance Indicator
MTC	Manufacturing Technology Connect
OEE	Overall Equipment Effectiveness
OEM	Original Equipment Manufacturer
PC	Personal Computer
SCM	Service Control Manager
SHDR	Simple Hierarchical Data Representation
SPC	Statistical Process Control
URL	Uniform Resource Locator
XML	eXtensible Markup Language
XSD	XML Schema Definition

1 INTRODUCTION

Production knowledge consists of understanding, organizing, and managing the machines, processes, and the tasks to be performed in a manufacturing facility. The focus of this paper

Michaloski, John; Proctor, Frederick; Venkatesh, Sid; Ly, Sidney; Manning, Martin.
"Automating Asset Knowledge with MTConnect."
Paper presented at the ASME International Manufacturing Science and Engineering Conference (MSEC), Blacksburg, VA, Jun 27-Jul 1, 2016.

will be on managing the machines, commonly referred to as assets. In an industrial context, asset management maximizes the performance of production resources for achieving manufacturing objectives – producing products faster, cheaper, and better. For shop floor equipment, this means having a clear understanding of how machines operate and how to improve manufacturing. Informative and timely asset management can be used to accurately assess manufacturing operation and to make adjustments to meet shifting manufacturing conditions. Example manufacturing roles for asset management include:

- accumulating resource knowledge for calculating accounting functions such as the actual machining cost of a part for bidding, and determining profits [1–4],
- identifying production bottlenecks [5–8],
- building up machine histories in order to perform predictive maintenance [9–12],
- incorporating equipment and process knowledge dynamically on a machine [13–15],
- recognizing excessively high asset utilization as a prerequisite to determining procurement needs [16–18].

Although timely machine status feedback during factory operation is not a complex concept, the collection and dissemination of the necessary status data in a timely and integrated manner has been a challenge within the discrete parts industries. The breadth of machines in the discrete industries is extensive, from additive and subtractive machine tools, robots, and automated guided vehicles (AGV). Plus, vendors, Original Equipment Manufacturers (OEMs), and end-users in the discrete industries have all been reluctant to adopt a global integration solution and instead prefer a proprietary approach. Clearly issues stem from the over–abundance of industrial standards from which to choose [19–26]. MTConnect is a standard to address many of these shortcomings, and is gaining traction in the discrete parts industry [27–29].

This paper discusses the automated collection and analysis of real-time machine status data based on the integration of MTConnect and machine status reporting. The second section gives a brief overview of MTConnect and the machine tool information model used for status reporting. The third section gives a background on ISO 22400 and its model of asset management. This section will include a mapping of MTConnect machine status into ISO 22400 asset management concepts. The fourth section describes a case study of asset management using MTConnect on the shop floor at a large aerospace factory. The final section contains a discussion on the benefits of machine tool status data in terms of support asset management as well as the problems encountered developing automated machine status feedback and the future work envisioned in this area.

2 MTConnect Overview

In order to reduce costs, increase interoperability, and maximize enterprise-level integration, the MTConnect specification has been developed for the discrete manufacturing industry [30]. Although aimed at solving the “Islands of Automation” problem prevalent in the discrete manufacturing industries, MTConnect is flexible and can be easily adapted to other asset management or other manufacturing applications [31]. MTConnect is a specification based upon prevalent Web technology including eXtensible Markup Language (XML) [32] and Hypertext Transfer Protocol (HTTP) [33]. Using this prevailing technology and providing free software development kits minimize the technical and economic barriers to MTConnect adoption.

Figure 1 shows the basic elements in an MTConnect solution. MTConnect “Agent” is a software process that acts as a bridge between a MTConnect “Device” and a Client Application. An MTConnect “Device” is a piece of equipment, like a CNC machining center or robot, organized as a set of components that provide data. MTConnect defines Events, Samples, Conditions, and Asset data items, whose XML format is all rigorously specified by XML Schema Definition (XSD) [34] schemas. Optionally, an MTConnect “Adapter” can be installed natively on the machine, which is a process that provides a communication link between a device and the agent. Agents can have a specialized remote Adapter or embedded “Backend” to communicate to the Device, (e.g., Simple Hierarchical Data Representation or SHDR [35] or OPC [36]).

The MTConnect standard defines XML schemas in order to exchange standard XML information. MTConnect defines the XSD content for Devices, Streams, Assets, or Errors necessary for retrieving factory device data, where:

- The MTConnect Devices XSD is an Information Model that describes each device and its data items available.
- The MTConnect Streams XSD is an Information Model that describes a time series of data items specified in the Devices XML including samples, events, and conditions.
- The MTConnect Error XSD defines the XML to describe one or more errors that occurred in processing an HTTP request to an MTConnect Agent.
- The MTConnect Asset XSD defines the XML pertaining to a machine tool asset, which is not a direct component of the machine and can be relocated to another device during its lifetime. The concept of MTConnect Asset refers to communication of resource asset knowledge and not the physical resource discussed in this paper. MTConnect Asset examples include tooling, parts, and fixtures.

Currently, MTConnect Agent supports four main types of requests:

- Probe request – response describes the devices whose data is being reported.

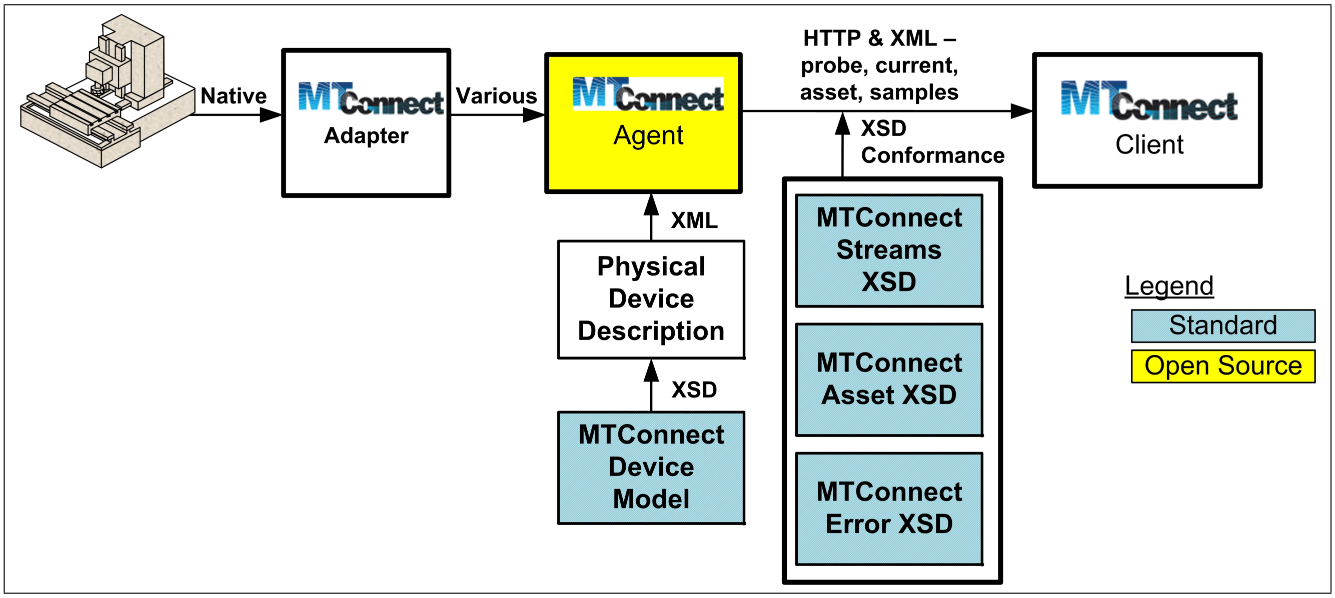


FIGURE 1: MTConnect Solution Overview

- Current request – retrieves the values of the devices data items at the point the request is received.
- Sample request – retrieves a list of past and/or current values for one or more data items.
- Asset request – retrieves data describing the state of an asset. Within an asset stream, there exists the ability to embed third party developed standards, (e.g., ISO 13399 [37]) within the response.

HTTP is the protocol used by MTConnect (as well as the World Wide Web) to define legal messages [38]. MTConnect also establishes what constitutes legal commands through the use of decorated Uniform Resource Locator (URL) such as http://agent.MTConnect.org/probe. MTConnect follows the rules of HTTP to fetch and transmit the requested MTConnect command, be it “probe”,“current”,“sample”, or “asset”.

In a “probe”, an MTConnect Device is modeled in XML which conforms to the Device XSD. The “Device Data Model” provides the Device(s) description that the world will see, which will typically be a subset of the total possible data from a device. The MTConnect Device model is not hardwired; rather users assemble an XML information model to match their device and their data requirements. Each MTConnect implementation uses a Device Data XML document to describe the data that will be conveyed from one or more devices. In effect, of the thousands of data items that may be available from a controller, MTConnect provides an XML document that enumerates which data items are in fact available. For example, suppose an MTConnect user is interested in the parameter “following error” of a servo drive, then the user would have to see if the Device is configured to supply “following error” data.

MTConnect Stream and Device XML Document are similar to all XML documents in that they are a tree representation. At the root, “Devices” define one or more “Device” (e.g., machine tool), which in turn defines a set of components, which in turn contain “Data Items”. Thus, an “MTConnect Device” is a machine organized as a set of components that provide data. Figure 2 shows a simple MTConnect hierarchy. In this MTConnect example, “cnc1” is composed of components: “power”, “controller”, and “axes”. Each component then has event or sample Data Item definitions. In this example, the “axes” component has sample data items: Srpm, Xabs, Yabs, and Zabs. In contrast, the “controller” component has two event data items: mode, and execution; and one sample data item: feedrate. Sample tags (e.g., Xabs, Yabs, Zabs) exhibit numerical values as strings. Some event tags have an enumeration string, e.g., the mode event can be either: MANUAL, MANUAL_DATA_ENTRY, AUTOMATIC.

Generally, MTConnect performance is low bandwidth (i.e., 1 to 2Hz), so that start/stop/program changes/alarms and other machine specific events are easily identified at this sampling rate. Higher bandwidth techniques are available in MTConnect, but are out of scope for this document.

3 ASSET MANAGEMENT

Manufacturing companies create products by converting raw materials, stock, or supplied goods into a finished product to sell. In general, manufacturing is complicated due to the parallel machine operation, dynamic job arrival, multi-resource require-

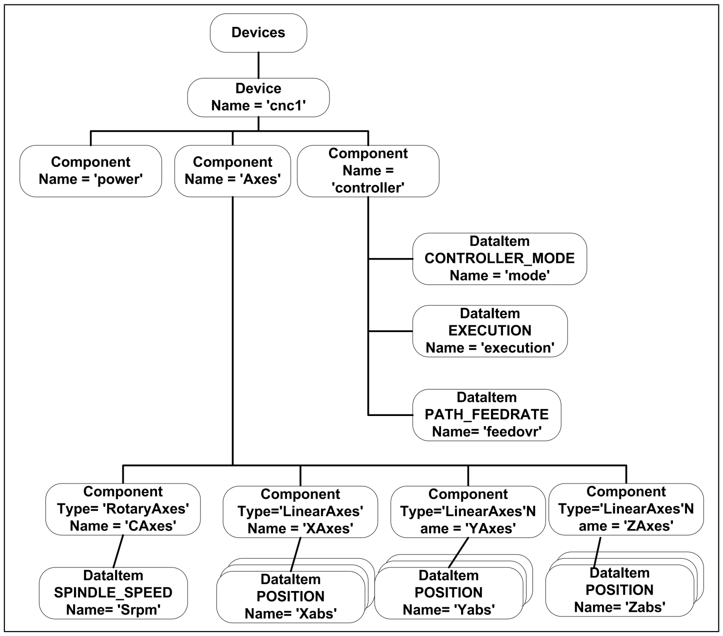


FIGURE 2: MTConnect Device Hierarchy Example

ments, and general job precedence constraints. At its most basic, manufacturing is handled by a set of machines, with a varying degree of flexibility and control; a material handling system that allows jobs to move between machines; and a set of computers for command and control. Preferably, the set of computers is all fully integrated on an enterprise network.

Asset management quantifies the performance of production resources in achieving manufacturing objectives. Asset management can be used to build up machine histories, which can be used to make informed business decisions, such as, capital avoidance (when to hold off on equipment purchases) or intelligent purchasing (formal evaluation of a given CNC model's actual performance, not anecdotal based on estimated data). Asset management can be used to store information on equipment within processes for use in undertaking corrective actions. The patterns of equipment operation can be analyzed for bottlenecks or underutilization and then used to improve the production process and reduce costs and improve product turnaround.

Depending on the individual or organization, possibly from different technical and geographic points of origin, assets may have a differing interpretation. Therefore, the consistent definition of an asset must be in place that is universally understood and adopted. Fortunately, the International Organization for Standardization (ISO) has established a manufacturing standard, ISO 22400 [39] "Automation systems and integration Key performance indicators (KPIs) for manufacturing operations management" that defines the concept of an asset and quantifies the associated performance metrics.

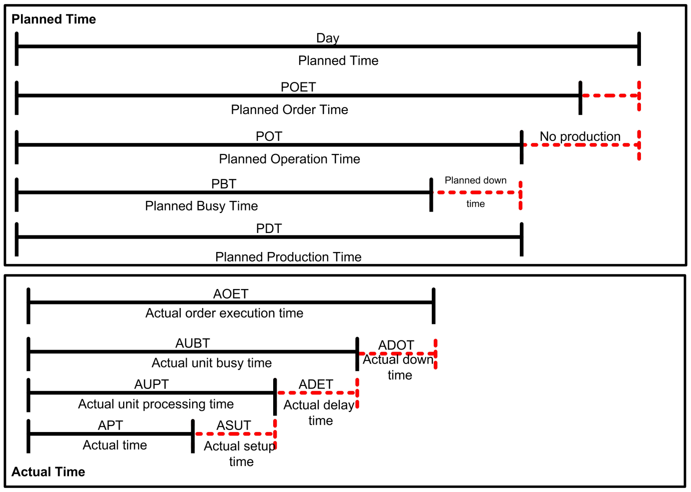


FIGURE 3: ISO 22400 Work Unit Formalism

Foremost, ISO 22400 offers consistent manufacturing concepts and terminology. Such that if KPIs are to be used in multiple locations and are to be searched, shared, and analyzed, a common vocabulary (as well as models) is a prerequisite. In addition, unnecessary cost from mistranslation, misunderstanding, and misinterpretation is avoided. Thus, common terminology and models are helpful in identifying and monitoring enterprise needs and outcomes by pooling data from multiple sources in a systematic method.

The ISO 22400 standard is presented according to high-level ISA 95 Manufacturing Operations Management (MOM) [40] information categories – the machinery and equipment, the product manufactured and its quality, the manufacturing personnel, the inventory, and other related manufacturing elements. Although ISO 22400 covers a complete production model, of interest to this paper is the ISO 22400 formalism to model individual assets or "Work Units" (i.e., ISA 88 terminology for resources or machines [41]) on the shop floor. ISO 22400 includes factors such as costs, quality, time, flexibility, environmental and social issues, and energy efficiency many of which are important but out of scope for this paper.

ISO 22400 formally breaks down the Work Unit production model into planned activities and actual production. Figure 3 shows the ISO 22400 formalism for "planned" and "actual" Work Unit modeling used to assess asset performance. ISO 22400 states that a day is the planned maximum time available for production and maintenance tasks, and a day depends on the number of shifts. In ISO 22400, OEE is calculated by the equations below:

$$\begin{aligned}
Availability &= PBT/PDT \\
&= PlannedBusyTime/PlannedProductionTime \\
Effectiveness &= (PTU \times PQ)/PDT \\
&= (Production\ time\ per\ unit \times Produced\ quantity)/PDT
\end{aligned}$$

$$Quality = PartCountGood/(PartCountGood + PartCountBad)$$
$$OEE = Availability \times Effectiveness \times Quality$$

In above equations, $Availability$, $Effectiveness$, $Quality$ and OEE units are percent. The $Availability$ determines how strongly the capacity of the machine for the value-added functions related to the planned availability is. $Availability$ takes into account planned time loss, e.g., meetings, coffee breaks, and maintenance. $Effectiveness$ is the measure for the efficacy of a process comparing target cycle time to the actual cycle time. $Effectiveness$ is also called efficiency factor or performance. The $Quality$ rate is the relationship of the proper quantity to the produced quantity. $Availability$ takes into account planned down time loss, $Effectiveness$ takes into account delays and speed loss, and $Quality$ takes into account part loss.

Unfortunately, OEE can be rendered meaningless due to the lack of appropriate data. Specifically, OEE requires a quality component in its calculation, which in discrete parts production is often impossible or can be difficult to determine since quality assessment is typically done later in the manufacturing process and is disconnected from the machining process. In this case OEE degrades into an asset utilization metric. For our analysis, we will assume quality is a meaningful component.

3.1 Mapping ISO 22400 to MTConnect

ISO 22400 distinguishes between performance data (such as Work Unit busy, delay, down, queued, etc.) and KPI (e.g., Work Unit OEE) [42]. It is the role of MTConnect to supply the machine status data. However, ISO 22400 is geared toward asset management with production flow between machines. In other words, ISO 22400 defines delay to include the concepts of blocked, starved, and queued as well as faulted or idle. For the case study that follows, a job shop is a more appropriate model of machine–part relationship and the concepts of blocked, starved, or queued are generally not relevant in a job shop part flow.

The terminology correspondence between ISO 22400 and MTConnect is not a perfect match, so it is best to clarify the data terminology. For ISO 22400, “Down” is the same concept as machine “Off” . Likewise the ISO 22400 concept of “Delay” incorporates the concepts “Idle” and “Faulted”. Long term “Faulted” effects the $OEE\ Availability$ of the machine, and would be a loss due to unscheduled maintenance. This leads to an ISO 22400 state model of down, idle, faulted, or busy while ignoring the starved and blocked states. (Idle as represented by the part queued state is a data parameter for a separate KPI.)

For MTConnect systems, the basic process to provide OEE performance data is to interpret MTConnect state logic using mode, execution, and other MTConnect tags to determine the machine status of busy, idle, faulted, and off. Although different, it is possible to map the MTConnect data into asset management state model. Table 1 shows the mapping of MTConnect status data items into state formalism corresponding to the ISO 22400 asset model. The MTConnect Data row (first row) details the expected raw data available from the MTConnect Device. The first column abbreviations (e.g., APT, ASUT, ADET) correspond to the ISO 22400 abbreviations from Figure 3.

TABLE 1: Mapping MTConnect State Data into Machine Status Data

Data	Parameters
MTConnect Data	Timestamp, Machine, Power, Mode, Execution, Spindle, Conditions, Feed override

Parameters	Data Mapping
APT ≡ Busy	$MTC_{program} \neq \emptyset\, and\, MTC_{execution} = Active$
ASUT ≡ Setup	$MTC_{mode} \in Manual$
ADET ≡ Delay	$MTC_{program} = \emptyset$ or $MTC_{execution} = Stopped\ or\ MTC_{execution} = Interrupted\ or\ MTC_{mode} = Manual\ or\ Faulted$
Down ≡ (Off)	$MTC_{power} = Off$
Faulted	$\exists\ MTC_{condition} = faulted\ until\ \forall MTC_{condition} \neq faulted$

Some of the OEE loss is not explicitly covered by ISO 22400. For example, $MTC_{feedoverride}$<100 % implies that the operator is slowing down machining and increasing cycle time, either to avoid chatter or for some other reason. This negatively impacts $OEE\ Effectiveness$ ratio. Another example of $OEE\ Effectiveness$ loss, that is not directly covered in ISO 22400, is if the operator is performing first part dry run testing, when spindle $rpm = 0$. Likewise the operator could be probing the part with machine axes moving but again spindle $rpm = 0$.

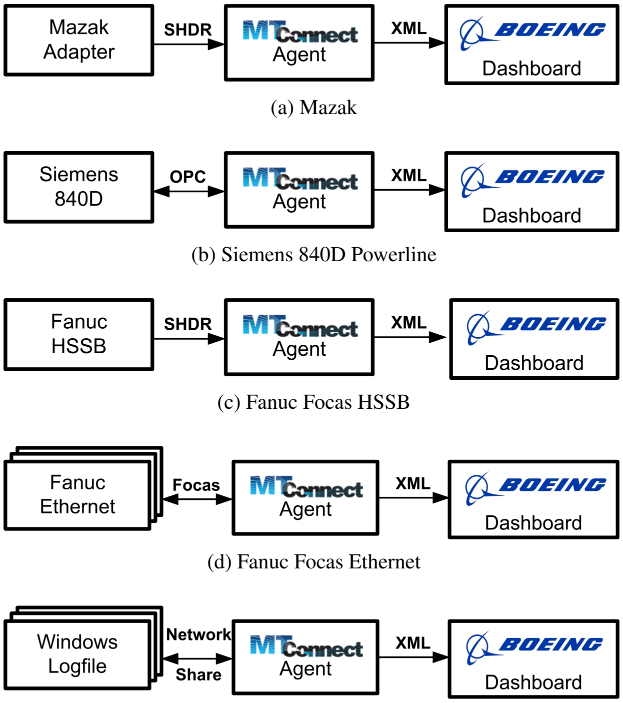
4 CASE STUDY

A case study was performed that investigates the MTConnect status data requirements for an aerospace manufacturing facility that produces a wide variety of airplane parts, (e.g., brackets, body joints, etc.). The Boeing Company Auburn facility is 195000 square meters (2.1 million-square-foot) and is reportedly the largest airplane parts plant in the world, making and storing more than 200000 parts for commercial jetliners [43]. Part materials vary and include aluminum, stainless steel, titanium, and inconel. The facility can produce parts ranging from a few ounces to over a ton, with dimensional control in the range of ±0.0254 mm to ±0.00254 mm (±0.001 inch to ±0.0001 inch). The disparity of part requirements means that there are many types of manufacturing machines, including horizontal mills, vertical mills, routers, waterjet, and wire electro discharge machining (EDM). For confidentiality, the actual performance data has been normalized; however, the analysis is representative of the data that is frequently encountered in facilities such as the one described in this study.

The flow of parts through the facility is determined by a workorder for each part(s). A process planner prepares a workorder for a part(s) that assigns resources, which incorporates constraints based on the asset configuration (e.g., 3 versus 5 axis), surface finish (e.g., high speed machining versus normal milling), machine horsepower, and feature tolerances, among a myriad of part requirements. At the same time the workorder is prepared, the corresponding part program based on the version and revision of the part is uploaded to the program database. The workorder is eventually routed to a machine operator, and in preparation uses one of the designated asset types, gets the raw material, downloads the part program from the database, and does a set up according to the workorder. Should the workorder specify that a large number of parts are to be made, a test try out is done on one part to insure correctness of the plan. Often after the test part is made, the part is inspected, and when the part meets or exceeds the quality requirements, the remainder of the parts are machined according to the workorder. This process is repeated until the test part satisfies the quality requirements. Overall, the flow of parts through the facility resembles a job shop, as opposed to a production line.

The Boeing Auburn plant has been an early adopter of MTConnect and has extensive MTConnect connectivity throughout the factory. The plant use of MTConnect, although not 100 %, encompasses a wide variety of machines and vendors: Mazak, Jomach, Northwood, DST, ATA Group, American Gesellschaft fr Fertigungstechnik und Maschinenbau (AGFM), and Nikon, as well as a variety of controllers: Original Equipment Manufacturer (OEM), Fanuc, Mitsubishi, and Siemens controllers. Most MTConnect Agents were installed as Windows Services that ran as a 24/7 operation. Since the MTConnect agents were a service and not application "exes", only the Windows Service Control Manager (SCM) can start/stop the programs. Whenever possible, native MTConnect solutions from the CNC vendor were preferred. However, this is not always possible, so custom MTConnect solutions were developed. Fortunately, MTConnect provides open source software solutions for the Agent and a wide range of Adapters, which can be found at `https://github.com/MTConnect`, and were used extensively.

Many of the implementations used an embedded MTConnect Adapter in the controller to perform the communication between a device and the agent (e.g., SHDR, Fanuc High Speed Serial Bus (HSSB) FOCAS). MTConnect also supported specialized "Backends" in the Agents to communicate to the device via some other remote access protocol, (e.g., OPC, Fanuc Ethernet FOCAS, Logfile). Below is a snapshot of some of the MTConnect solution strategies employed.



(a) Mazak

(b) Siemens 840D Powerline

(c) Fanuc Focas HSSB

(d) Fanuc Focas Ethernet

(e) Logfile

FIGURE 4: MTConnect Case Study Solutions

- Mazak provides native MTConnect support, supplying a SHDR Adapter and MTConnect Agent. Installation of the MTConnect components were handled by a Mazak service representative. Figure 4a shows the Mazak controller emitted SHDR data to the MTConnect Agent, which translated the data updates into XML.
- Dörries Scharmann Technologie (DST), Jomach, and Echospeed CNC machines, use a Siemens 840D controller. The older Siemens 840D (i.e., Powerline models) support OPC Data Access "Classic" [44]. Figure 4b shows two-way OPC communication using customized MTConnect Agent software with an OPC adapter backend. Heightened cybersecurity precautions make the use of traditional OPC with Distributed Component Object Model (DCOM) connection very problematic.
- Northwood, Cincinnati, Heian Router, and numerous contour tape laying machines (CTLM) used a Fanuc controller. There were many different Fanuc iSeries controller models with subtle differences in functionality. Fanuc machines required the FANUC OpenFactory CNC API Specifications

(Focas) library to communicate to the controller. Focas provides a DLL with API to manage and query the state of the CNC machine. Fanuc supplies two communication methods using Focas: High Speed Serial Bus (HSSB) and Ethernet. Figure 4c shows the HSSB Focas solution, where one Focas SHDR Adapter is installed on each CNC and then an MTConnect Agent reads the Fanuc CNC data items using the SHDR protocol. Figure 4d shows the Ethernet Focas solution, which allows MTConnect to remotely access status of multiple controllers.

- For ATA Group, AGFM, and Nikon Coordinate Measuring Machines, status data was obtained from the controller log file. Figure 4e shows a Windows networked file sharing approach used in conjunction with controller log file monitoring. The networked file sharing approach is an easy deployment method as the controllers do not require any special software interface, and need not be aware of the MTConnect monitoring. Cybersecurity protection prevented traditional file access as even file sharing from the MTConnect service across the network needed logon authentication.

Cybersecurity and safety protection of the machines and humans are major concerns. Two cybersecurity schemes were in place. One scheme has a dual Ethernet solution where the MTConnect Agent runs on a front end Personal Computer (PC) and talks to the asset through a local network connection. The second scheme uses a hardware firewall on the machine to block any network traffic, except from the computer running an MTConnect Agent. In each case the goal is to isolate the machine from the corporate Intranet but still allow connectivity by MTConnect.

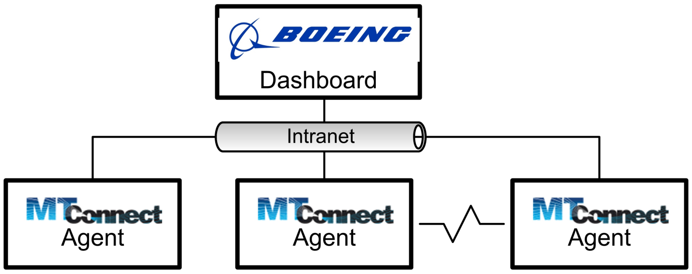


FIGURE 5: Dashboard Client Application Architecture

A stack light dashboard client application monitored enterprise as well as the case study factory machine status in real-time. Figure 5 shows the dashboard architecture, which is a centralized, Web-based software application that collects machine status data from a large collection of MTConnect agents scattered throughout the enterprise, not just at the Auburn facility. All the MTConnect agent front-ends were nearly identical, while the dispersed assets themselves were wide-ranging with varied functionality. All machine status data was gathered using MTConnect using the Intranet as the communication backbone. Managers can visually see which machines are up as well milling and get an intuitive feel for factory performance. With some historical logging of the factory dashboard performance and drilling down on the actual use of a set of machines, one can perform asset management with real data.

Previous to MTConnect networking of assets, machine status monitoring would have to be done manually. Manual data collection is error prone and sporadic. Moreover, with an automated process, operators are able to spend less time on non-value added reporting activities and more on productivity-oriented tasks. However, this automated approach must be easy to integrate or the benefits will never materialize.

The goal for Auburn and other world class discrete manufacturers is to achieve an 85 % OEE. Numbers higher than 85 % could indicate a bottleneck. When MTConnect asset management is used in conjunction with real time production log files, actionable knowledge is garnered where bottlenecks can be determined so that resources can be directed to mitigating the problem. Numbers lower than 85 % indicate lost productivity. A simple example illustrates the lost revenue that is identifiable with real OEE values [45]. To determine a part *BuildTime* given the asset OEE:

$$BuildTime = Idea\ Cycle\ Time/OEE$$

where *Ideal Cycle Time* is the time required to produce the product if the asset was producing at 100 % of planned OEE capacity. Assuming an Ideal Cycle Time 270 minutes leads to the equations:

$$\begin{aligned} BuildTime &= 270/.85 \\ &= 317\ minutes \\ BuildTime &= 270/.50 \\ &= 540\ minutes \end{aligned}$$

If we assume a machine burn rate of $1000 per hour, a loss of approximately 2 hours equates to $2000.

OEE done with MTConnect asset management also helps provide hard numbers when assessing capital expenditures. An accurate OEE can determine asset capacity when combined with actual customer demand for product based upon planned production time (PDT). Capacity will vary based upon the utilization of the asset which changes based on the PDT or Planned Production Time (i.e., number of shifts per day, number of days per week, breaks, holidays, etc.). Assuming a baseline PDT capacity of 3 shifts/day reduced by breaks yielding 20.4 hours per day total that will be further limited by the OEE reflected in the BuildTime:

$$CurrentCapacity\ (CC) = PDT/BuildTime$$

$$
\begin{aligned}
.85 \times OEE &= 1224\ min/317\ min \\
&= 3.8\ parts/day \\
.50 \times OEE &= 1224\ min/540\ min \\
&= 2.2\ parts/day
\end{aligned}
$$

Assuming a 30 day month and the customer wants 90 parts a month, then if the OEE is 0.50 % additional assets will be required to satisfy the customer needs. Likewise, using a similar approach, an anticipated increase in part demand can be strategically planned to see if current capacity coverage is sufficient. One of the primary benefits of quantifying asset performance is cost avoidance.

5 Discussion

Asset management is the monitoring of machine operation to quantify performance for manufacturing. The key goals of asset management include trouble-free integration within the enterprise, collection and management of asset OEE information, real-time monitoring for preventive and reactive maintenance, and introspective process monitoring for adaptive control and error compensation. To attain a goal of automated asset management, MTConnect has been shown as a standard and facilitated an automated way to integrate discrete factory floor machines into the enterprise.

This paper detailed the use of MTConnect at a large aerospace facility. MTConnect is an open factory communication standard that leverages the Internet and uses XML for data representation. Reliance on dominant and standard technology made integration easier. Deployment did include custom approaches to integrating assets. These custom approaches leveraged MTConnect open source solutions available for many controller models. In addition, third party integrators provide affordable MTConnect solutions for a number of controllers. In spite of the benefits, CNC vendor support for MTConnect varied, so complete integration of MTConnect on all factory machines remains challenging.

Once integrated, asset management can be performed by collecting machine status data. Traditionally, manual recording of activities is used to assess productivity. The use of real-time machine status and recorded historical activity are important developments in the quest for improving manufacturing. Using real-time and historical data, one can verify that the machine utilization is running as expected and if not, actionable procedures can be identified and undertaken.

One final caveat is in order. Measured OEE is necessary, but not sufficient, in order to enact production improvements. Understanding the type and severity of delays within production is required to remediate process problems and improve OEE. MTConnect can offer insight into some of the delays associated with an asset. Such problems can include the under-performing operator, difficult setup, or chatter among numerous potential troubles, which can require further examination to truly understand the root cause. Clearly hard real data can be beneficial in understanding the manufacturing process. Informed management can make better decisions based on facts not guesses, which leads to better manufacturing.

In the discrete part industry, integrating enterprise assets through their automated data collection is a daunting task. Automated factory data collection using MTConnect need not be contained to simple asset management. Expanding the scope to include advanced asset techniques, such as prognosis and condition based health monitoring, are possible given improved data collection. However, just collecting the data may not be sufficient, as a results-driven, automated analysis of an asset is imperative to taming the potential voluminous windfall of data. In addition, even simple asset management could benefit from automated analysis and decision making, as automated and integrated data collection in itself does not make an intelligent system.

Disclaimer

Commercial equipment and software, many of which are either registered or trademarked, are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by Boeing or the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

REFERENCES

[1] Stockton, D., Khalil, R., and Mukhongo, M., 2013. “Cost model development using virtual manufacturing and data mining: Part I - methodology development”. *International Journal of Advanced Manufacturing Technology,* ***66***(5-8), pp. 741 – 749.

[2] Ben-Arieh, D., and Lavelle, J. P., 2000. “Manufacturing cost estimation: Applications and methods”. *Journal of Engineering Valuation and Cost Analysis,* ***3***(1), pp. 43 – 55.

[3] Sormaz, D., Gannon, P., and Pulugurta, S., 2013. “Methodology for feature modeling and cost estimation of large cast parts”. In IIE Annual Conference and Expo 2013, pp. 2349 – 2356.

[4] Jung, J.-Y., 2002. “Manufacturing cost estimation for machined parts based on manufacturing features”. *Journal of Intelligent Manufacturing,* ***13***(4), pp. 227 – 238.

[5] Dewa, M., and Chidzuu, L., 2013. “Managing bottlenecks in manual automobile assembly systems using discrete event simulation”. *South African Journal of Industrial Engineering,* ***24***(2), pp. 155 – 166.

[6] Lenort, R., Klepek, R., Wicher, P., and Besta, P., 2013. "A methodology for determining and controlling the buffers before floating bottlenecks in heavy machinery production". *Metalurgija,* ***52***(3), pp. 391 – 394.

[7] White, T., Sengupta, S., and Vantil, R. P., 2012. "A new way to find bottlenecks". *Industrial Engineer,* ***44***(11), pp. 45 – 49.

[8] Lin, L., Qing, C., Guoxian, X., and Ambani, S., 2011. "Throughput bottleneck prediction of manufacturing systems using time series analysis". *Journal of Manufacturing Science & Engineering,* ***133***(2), pp. 021015–1 – 021015–8.

[9] Araiza, M. L., 2004. "A formal framework for predictive maintenance". In AUTOTESTCON (Proceedings), pp. 489 – 495.

[10] Susto, G. A., Wan, J., Pampuri, S., Zanon, M., Johnston, A. B., O'Hara, P. G., and McLoone, S., 2014. "An adaptive machine learning decision system for flexible predictive maintenance". In IEEE International Conference on Automation Science and Engineering, Vol. 2014-January, pp. 806 – 811.

[11] Ciocoiu, L., Hubbard, E.-M., and Siemieniuch, C. E., 2015. "Implementation of remote condition monitoring system for predictive maintenance: An organisational challenge". In Contemporary Ergonomics and Human Factors 2015, pp. 449 – 453.

[12] Sipos, R., Fradkin, D., Moerchen, F., and Wang, Z., 2014. "Log-based predictive maintenance". In Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1867 – 1876.

[13] Deshayes, L., Welsch, L., Donmez, A., Ivester, R., Gilsinn, D., Rhorer, R., Whitenton, E., and Potra, F., 2006. "Smart machining systems: issues and research trends". In *Innovation in Life Cycle Engineering and Sustainable Development*, D. Brissaud, S. Tichkiewitch, and P. Zwolinski, eds. Springer Netherlands, pp. 363–380.

[14] Suh, S., Kang, S., Chung, D., and Stroud, I., 2008. *Theory and Design of CNC Systems*. Springer Series in Advanced Manufacturing. Springer London.

[15] Grabowski, R., Denkena, B., and Köhler, J., 2014. "Prediction of process forces and stability of end mills with complex geometries". *Procedia CIRP,* ***14***, pp. 119–124.

[16] Leitner, K.-H., 2011. "The effect of intellectual capital on product innovativeness in SMEs". *International Journal of Technology Management,* ***53***(1), pp. 1–17.

[17] Chen, Y.-S., and Chen, B.-Y., 2009. "Using data envelopment analysis (DEA) to evaluate the operational performance of the wafer fabrication industry in taiwan". *Journal of Manufacturing Technology Management,* ***20***(4), pp. 475 – 488.

[18] South African Institute of Electrical Engineers, 2003. "IT in manufacturing". *Elektron,* ***20***(4), pp. 48 – 49.

[19] International Organization for Standardization (ISO), 2003. *ISO 11898-1:2003 Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signalling*.

[20] International Electrotechnical Commission (IEC), 2003. *IEC 61158 Type 2 - EtherNet/IP: Communication Profile Family 2*.

[21] International Electrotechnical Commission (IEC), 2014. *IEC 61158 Type 10 - PROFINET: Communication Profile Family 3*.

[22] International Electrotechnical Commission (IEC), 2014. *IEC 61158 Type 23 - CC-Link IE: Communication Profile Family 8*.

[23] International Electrotechnical Commission (IEC), 2014. *IEC 61158 Type 12 - EtherCAT: Communication Profile Family 12*.

[24] International Electrotechnical Commission (IEC), 2014. *IEC 61158 Type 13 - Powerlink: Communication Profile Family 13*.

[25] International Electrotechnical Commission (IEC), 2014. *IEC 61158 Type 15 - Modbus-TCP: Communication Profile Family 15*.

[26] Czech National Standard European Standard, 2002. *CSN EN 50325 - Industrial communications subsystem based on ISO 11898 (CAN) for controller-device interfaces*.

[27] Modern Machine Shop. Data-driven manufacturing moves ahead at mazak. `www.mmsonline.com/articles/data-driven-manufacturing-moves-ahead-at-mazak`. [Online; accessed 20-Nov-2015].

[28] Okuma America. MTConnect. `www.okuma.com/mtconnect`. [Online; accessed 20-Nov-2015].

[29] Mazak. MTConnect. `www.mazakusa.com/machines/mtconnect/`. [Online; accessed 20-Nov-2015].

[30] MTConnect Institute. MTConnect Specifications. `www.mtconnect.org/standard`. [Online; accessed 25-Sept-2015].

[31] Edstrom, D., and Leonard, S., 2013. *MTConnect: How and Why a Royalty-Free and Open-Source Standard Is Revolutionizing the Business and Technology of Manufacturing: to Measure Is to Know*. WordStyle LLC.

[32] World Wide Web Consortium, 2006. Extensible markup language (XML) 1.0 (fourth edition).

[33] The Internet Society, 1999. Hypertext transfer protocol - http/1.1.

[34] World Wide Web Consortium, 2004. XML schema part 0: Primer second edition. `www.w3.org/TR/2004/REC-xmlschema-0-20041028`. [Online; accessed 20-Nov-2015].

[35] Sobel, W. MTConnect Standard SHDR Protocol Companion Specification. `https://github.com/mtconnect/adapter/blob/master/MTC_SHDR.docx`. [Online; accessed 25-Sept-2015].

[36] OPC Foundation. OPC. `https://opcfoundation.org`. [Online; accessed 25-Sept-2015].

[37] International Organization for Standardization, 2014. *ISO 13399, Cutting tool data representation and exchange*. Geneva, Switzerland.

[38] MTConnect User Portal. MTConnect HTTP Primer. `mtcup.org/wiki/HTTP_Primer`. [Online; accessed 25-Sept-2015].

[39] International Organization for Standardization (ISO), 2014. *ISO 22400-1:2014: Automation systems and integration Key Performance Indicators (KPIs) for manufacturing operations management Part 1: Overview, concepts and terminology*. Geneva, Switzerland.

[40] ISA, 2005. *ANSI/ISA-95.00.03-2005, Enterprise-Control System Integration, Part 3: Models of Manufacturing Operations Management*. International Society of Automation.

[41] ISA, 2010. *ANSI/ISA-88.00.01-2010 Batch Control Part 1: Models and Terminology*. International Society of Automation.

[42] International Organization for Standardization (ISO), 2014. *ISO 22400-2:2014: Automation systems and integration Key Performance Indicators (KPIs) for manufacturing operations management Part 2: Definitions and descriptions*. Geneva, Switzerland.

[43] KOMO Television. Boeing's Auburn plant declared safe. `www.komonews.com/news/boeing/27937709.html`. [Online; accessed 20-Nov-2015].

[44] OPC Foundation. OPC Data Access Classic. `opcfoundation.org/developer-tools/specifications-classic/data-access/`. [Online; accessed 20-Nov-2015].

[45] Salter, J., 1998. Overall equipment effectiveness (OEE). Tech. rep., Boeing Company.

CAVITY OPTICAL TRANSDUCER PLATFORM WITH INTEGRATED ACTUATION FOR MULTIPLE SENSING APPLICATIONS

Thomas Michels[1], and Vladimir Aksyuk[1]*

[1]Center for Nanoscale Science and Technology, National Institute of Standards and Technology, Maryland, USA

ABSTRACT

We present an on-chip cavity optomechanical transducer platform that combines high measurement bandwidth and very low displacement noise floor with compactness, robustness, small size, and potential for low cost batch fabrication inherent in micro-electro- mechanical- systems (MEMS) [1]. Our fiber-pigtailed transducers use surface-micromachined silicon-on-insulator photonic, low-stress silicon nitride structural and metal electrical actuation layers, while front- and backside bulk micromachining defines v-grooves and overhanging cantilevers. The motion of the mechanical devices, such as cantilevers and high mechanical quality factor membrane resonators, is optically measured by integrated silicon micro disk optical cavities. The devices can be actuated electrothermally or electrostatically, and this actuation can also be used to tune readout gain. A displacement noise floor below 10 fm/√Hz is achieved for mechanical devices with stiffnesses varying over three orders of magnitude (≈ 0.2 N/m to ≈ 200 N/m). The combination of electrical actuation, low-loss mechanics, and optomechanical readout will enable a wide variety of high-performance on-chip resonant and non-resonant sensors.

INTRODUCTION

The measurement of physical quantities by transducing them to a mechanical motion has a long history. The recent advancements in fabrication of micro- and nanomechanical resonators have continued this trend. Ongoing miniaturization and better process control have enabled high quality factors for both optical and mechanical resonators and therefore more sensitive measurement of microscopic physical phenomena. While micromechanical pressure and acceleration sensors are now ubiquitous in consumer electronics and other products of everyday life, in the physics laboratory the micro- and nanoscale resonators allow measurements with unprecedented degree of precision [2].

One of the most significant obstacles to realizing the full potential of micro- and nanomechanical sensing is the readout of the motion of the small resonator with high sensitivity, high bandwidth, and without excess power dissipation. In the past years numerous methods for the readout of resonator motion have been developed [3]. Electrical readout schemes, such as capacitive, magnetomotive, piezoresistive, and piezoelectric, are convenient but suffer from various combinations of poor scaling with reduced size, power dissipation limitations, magnetic field and material requirements, and thermal Johnson noise in the readout signal. On the other hand, optical readout schemes, such as beam deflection and interferometric, substitute optical shot noise for thermal noise, in principle don't dissipate any power at the transducer, and have a high measurement bandwidth. However, to effectively couple motion to light, most of the off-chip optical methods need a certain minimum moving structure size and reflectivity, which often involves bulky structures or mechanically dissipative reflective coatings.

In nanophotonic optical cavities, the light is trapped in a very small volume and is made to interact for a longer timer and more closely with the mechanical resonator. Typical photonic cavity optical quality factors on the order 10^5 to 10^6 increase the readout signal to noise by the same factor. The readout bandwidth is reduced from ≈ 100 THz optical frequency to about ≈ 100 MHz, still fast enough for most mechanical sensors. Maintaining stable coupling of a microscopic mechanical resonator with an off-chip optical cavity is challenging due to alignment and drift of components with respect to each other. Here this challenge is overcome by integrating the high quality factor optical cavity directly underneath the moving device, allowing strong interaction with the optical near-field of the cavity, while avoiding mechanical contact (Fig.1). This interaction is described by the optomechanical coupling coefficient (g_{OM}) relating the change in optical frequency of the micro disk cavity to the displacement of the mechanical device. This fully integrated stable and practical optomechanical transducer is fiber connectorized and implements the readout of mechanical motion with gigahertz bandwidth.

Low loss, stable and robust fiber coupling of the transducer is essential to allow sensitive and reliable operation. Therefore, the fibers have to be securely attached to the chip without the introduction of high excess losses between the on-chip waveguide and the optical fiber.

This readout approach allows independent tailoring of the various optical and mechanical parts of the transducer. The photonics can be separately optimized for low losses, high quality factor and desired cavity size, while tuning the waveguide-cavity coupling depth and the optomechanical coupling to achieve the optimal readout sensitivity and dynamic range. The mechanical components' size, shape, stiffness, and resonance frequency can be tailored to best address the specific sensing applications. The actuation can be tailored for the needed displacement and force ranges, ideally without introducing mechanical losses, avoiding increased mechanical noise and decreased Q in resonators.

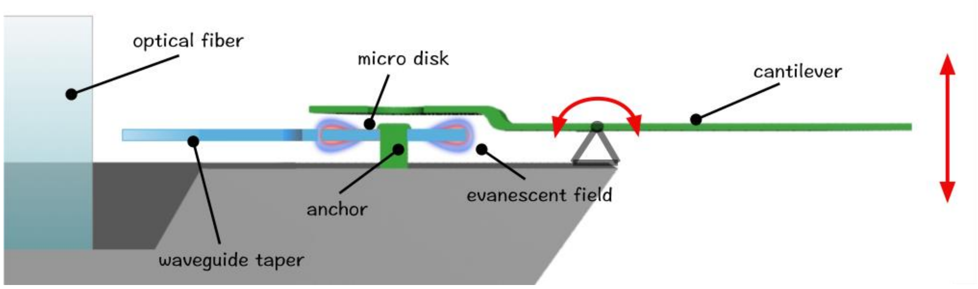


Figure 1: Exemplary schematic of the transducer (not to scale) showing overhung cantilever on a torsional pivot as the mechanical device. SiN is shown in green, Si is shown in blue and grey. The red arrow indicates the direction of movement.

Michels, Thomas; Aksyuk, Vladimir.
"Cavity optical transducer platform with integrated actuation for multiple sensing applications."
Paper presented at the Solid State Sensor, Actuator and Microsystems Workshop, Hilton Head Island, SC, Jun 5-Jun 9, 2016.

TRANSDUCER PLATFORM COMPONENTS AND DESIGN

Figure 1 schematically illustrates the arrangement of the different components in our transducer platform, such as the optical fiber, inverse-taper coupler, waveguides, microdisk cavity, and the mechanical (torsional cantilever) structure. Electrically-controlled actuators (not shown) are also included in the platform to tune the static position and dynamically excite the motion of the mechanical device. The photonic structures for operation in the telecommunication wavelength range are fabricated in the silicon device layer of a silicon-on-insulator (SOI) wafer, because of the outstanding optical and mechanical properties of silicon. The mechanical device is created in silicon nitride (SiN), because it shows good mechanical properties resulting in high quality factor devices, has low optical loss, an index of refraction below that of Si and is compatible with a hydrofluoric (HF) acid release. For the metallization we choose gold with a chromium adhesion layer (Cr/Au), compatible with HF and potassium hydroxide (KOH) etches. Furthermore, the combination of SiN and Cr/Au shows a good thermal bimorph actuation efficiency. Silicon dioxide is used as the sacrificial material.

The sensitivity to motion is proportional to the optical quality factor of the micro disk cavity and quickly increases with decreasing gap between the cavity and the mechanical resonator [1]. It is therefore important to accurately locate the mechanical structure in close proximity to an optical micro disk cavity, while maintaining the high optical quality factor of the micro disk optical mode. In our design, the micro resonator is lithographically aligned to the disk, and completely encloses it, while a sacrificial layer defines the gap in the fabrication process. Dedicated lithography and etch steps are used to reduce the sacrificial layer thickness to a predetermined value at the optomechanical transducer, allowing us to control the gap within tens of nanometers, while keeping a thicker silicon dioxide sacrificial and cladding layer elsewhere

Coupling light from optical fiber to an on-chip waveguide may result in high losses due to mode-size and effective-index mismatch between the optical fiber and the Si waveguide structure, which induce optical scattering and backreflection. Tapering from the waveguide dimensions to the fiber mode dimensions for improving coupling efficiency between optical- fiber and waveguide modes have been suggested [4]. However, to avoid excessive coupling to radiation modes in the taper the required typical taper length must be of the order of a millimeter. Inverse tapers, decreasing the waveguide width at the end accomplish low loss coupling by expanding the waveguide mode to match the fiber mode size. Almeida suggested a micrometer- long nanotaper coupler that converts both the mode size and the effective index of the waveguide to that of the optical fiber [5]. The nanotaper is fabricated in the silicon device layer of a SOI wafer and is butt coupled to the optical fiber. In this coupling scheme, the optical fiber has to be no more than a few micrometer away from the tapered waveguide end. However, it is difficult to fix the optical fiber in the optimum position for the best coupling, without any support structure. Therefore, we etched v-grooves into our chip to be able to actively align and securely attach the optical fibers in the optimum optical coupling position with UV curable epoxy. Since the mode size and effective index of the taper strongly depend on the surroundings of the nanotaper we decided to use an overhanging silicon nanotaper in air, avoiding the possibility of increased losses into the nearby substrate. Simulations were performed to maximize the mode size and effective index overlap and therefore the coupling efficiency. All simulations were performed at $\lambda = 1.55$ µm. As input mode reference, a Gaussian beam with the diameter of a single mode optical fiber was used. The waveguide core material was Si (refractive index of silicon used: $n_{Si} = 3.48$). The waveguide height and width were taken as $h = 260$ nm and $w_w = 500$ nm, respectively. The transmission (S_{21}) has been calculated for TE- and TM- like modes. A parametric sweep has been performed to find the optimal taper tip width, which gives the best optical transmission and can still be fabricated within the presented process without more than 5 % deviation from the ideal geometry. Fig. 2 shows the results for S_{21} as a function of taper tip width. The maximum transmission occurs at a taper tip width of around ≈ 100 nm, which is also a reasonable size for the electron beam lithography used to define the waveguide taper. The taper nominal length is ≈ 50 □m.

Separating photonic and mechanical layers affords flexibility in the design of the mechanical parts to suit specific sensing applications. We designed cantilever structures, torsional structures, and membranes, on chip structures, and overhanging structures, as well as various types of actuation mechanisms. The membrane structures are designed to have a resonance frequency ranging from ≈ 70 kHz up to ≈ 1 MHz - an SEM of these sensors is embedded into the setup in Figure 3. The cantilevers are designed to combine small size with high resonance frequencies, with a range between ≈ 50 kHz and ≈ 4 MHz. The integration of an actuator increases the range of possible applications. The built-in static actuation gives the possibility of tuning the transducer gain and measurement range. This is accomplished by changing the static gap size between the mechanical structure and the optical cavity. We decided to develop designs for two actuations schemes, bimorph and electrostatic actuation. Bimorph actuators deliver fast responses and large force. However, the introduction of metal on the mechanical structure creates significant internal losses and therefore reduces the mechanical quality factor drastically. In contrast, electrostatic fringe field actuation doesn’t need any metal in contact with the mechanical member, which lets the mechanical member freely oscillate and doesn’t affect the mechanical quality factor. However, the maximum forces, as indicated by simulation, are rather small, but still suitable for on-resonance excitation for frequency sensing. Detailed actuator performance is a subject of a future study.

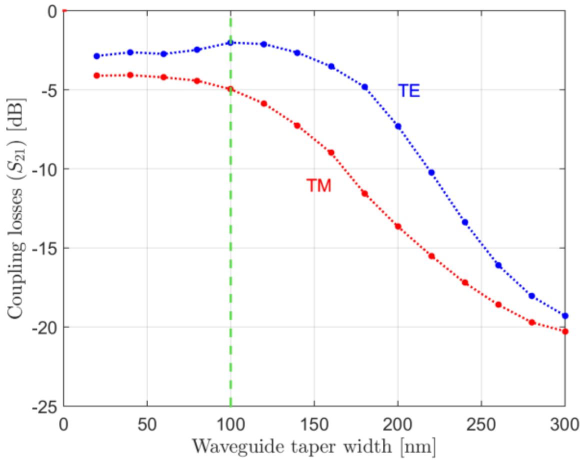


Figure 2: Simulation result of the transmission (S21) as a function of taper tip width. The inverse taper length is 50 □m.

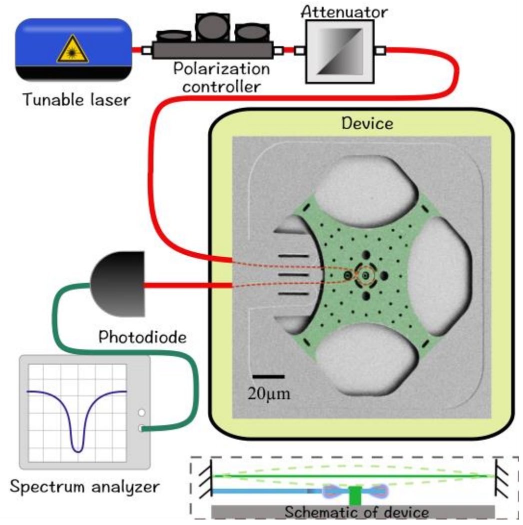


Figure 3: Schematic of the detection setup with an embedded SEM of the membrane transducer and a cross section schematic for this transducer (dashed box).

DEVICE FABRICATION

The main challenge is to fabricate these diverse optical and mechanical structures in a unified batch fabrication process and a single platform, which can be tailored for specific applications. In the following we will present the process using the overhanging cantilever probe as an example.

The fabrication for the cavity optical transducer is based on double side polished SOI 100mm (4”) wafers with a ≈ 260 nm top silicon layer, with low doping for good optical properties, and a ≈ 2 µm buried oxide (BOX) layer. The process flow is summarized in Figure 4. In the first step, the waveguide taper, waveguide, and micro disk are defined via electron beam lithography and inductively-coupled reactive ion etching down to the BOX layer. The nominal width of the waveguide is ≈ 500 nm and the gap between the waveguide and the disc is defined to be ≈ 340 nm. The waveguide is linearly tapered down to a width of 100 nm over the distance of ≈ 50 µm at both waveguide ends for low loss coupling to/from optical fibers (Fig. 4 b). The remaining structures are defined by i-line stepper optical lithography unless otherwise noted. A sacrificial silicon oxide layer (≈ 1 µm) is deposited and defined to create a window to the Si substrate for the later KOH etching as well as a hole in the center of the micro disk, which is used to anchor the micro disk to the bulk silicon with the following SiN layer. The silicon dioxide is thinned down by a CF$_4$ plasma etch through a lithographically-defined window in photoresist in the region above the micro disk to ensure good optomechanical coupling (Fig. 4 c, d). A low-stress silicon nitride layer (≈ 400 nm) deposited in a low-pressure chemical-vapor deposition furnace acts as a passivation layer in the waveguide region and as structural material for the mechanical structure. Following nitride deposition, a gold layer is deposited and defined in a liftoff process to create a micro heater, electrical connection, and wire bond pads. (For the electrostatically actuated transducer, the micro heater is replaced by electrodes for fringe field actuation). The SiN layer is lithographically patterned (Fig. 4 e), and dry etched to form the SiN cantilever, SiN ring above the micro disk, and SiN anchor to mechanically attach the micro disk to the bulk silicon. The previously defined metal layer is used as a hard mask for SiN, to self-align the SiN structure in critical areas (Fig. 4 e). For front side protection during the later KOH etch, a hafnium oxide (HfO) layer of ≈ 20 nm is deposited via atomic layer deposition.

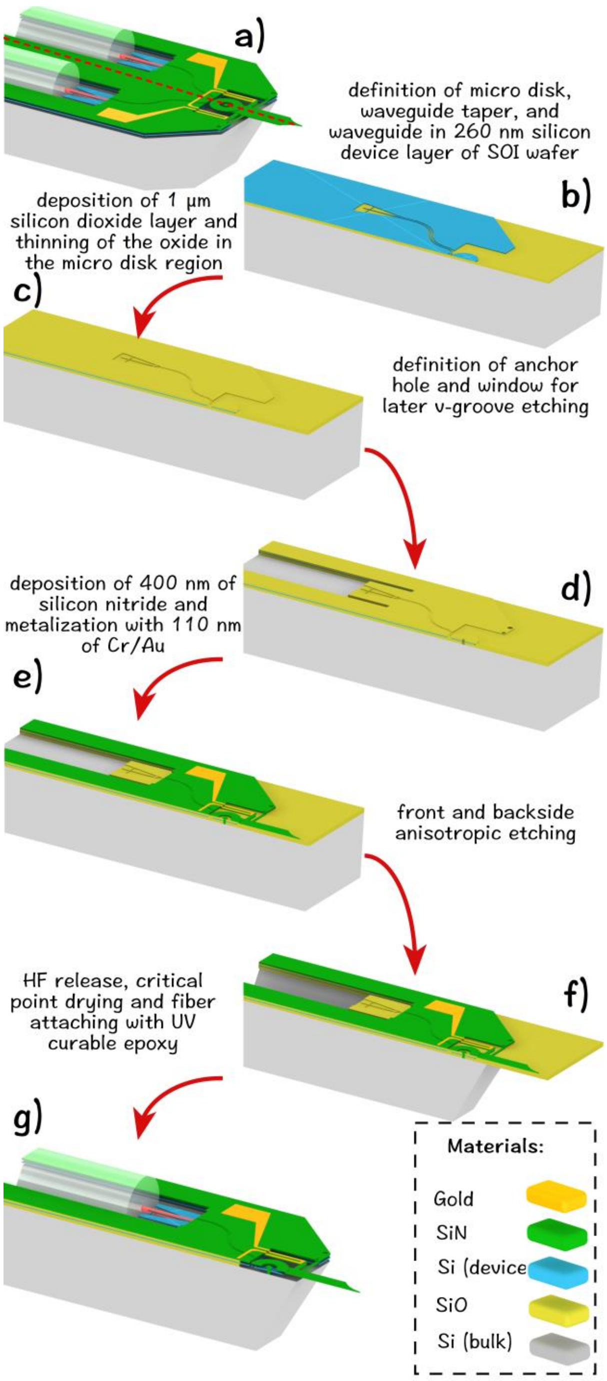

a)
definition of micro disk, waveguide taper, and waveguide in 260 nm silicon device layer of SOI wafer
b)
deposition of 1 µm silicon dioxide layer and thinning of the oxide in the micro disk region
c)
definition of anchor hole and window for later v-groove etching
d)
deposition of 400 nm of silicon nitride and metalization with 110 nm of Cr/Au
e)
front and backside anisotropic etching
f)
HF release, critical point drying and fiber attaching with UV curable epoxy
g)
Materials:
Gold
SiN
Si (device
SiO
Si (bulk)

Figure 4: Representation of the process flow for the transducer with integrated thermal actuation and overhanging tip. The image in the top left shows the whole device. The dashed red in indicates the path for the cross sectional views (a).

In the following, a reactive ion etch (RIE) is used to open up a window in the HfO and SiN for anisotropic etching of the silicon, to form v-grooves for optical fibers. A back to front aligned backside lithography followed by RIE etching is used to form an anisotropic etch window on the backside as well. Both lithographies for the definition of the front and back side etch window for anisotropic etching are defined with contact aligner lithography. During the following anisotropic silicon etch, v-grooves are formed on the front side of the chip and the shape of the cantilever chip is defined by etching through the handle wafer from the backside (Fig. 4 e). (Another approach is the replacement of the backside KOH etch with a ICP etch to create a backside trench with vertical sidewalls. This approach has been used to develop acceleration sensors with large seismic masses made from the handle wafer.) Silicon dioxide layers and HfO are removed by 49 % HF wet etching to undercut and release the movable structures as well as the micro disk, which is anchored to the bulk silicon with a SiN anchor. A critical point drying process is used to avoid stiction between the parts due to capillary forces (Fig. 4 f). At the end of each v-groove the overhanging waveguide inverse tapers are suspended between silicon support structures and coupled to optical fibers, which are placed in the v-groove, actively aligned and glued into place with ultraviolet (UV) light curable epoxy.

MEASUREMENT SETUP

The detection setup used to characterize the device is shown in Figure 3. Light from a tunable laser (1520 nm to 1570 nm) is sent through a polarization controller and coupled into the fiber pigtailed device, allowing for polarization adjustment to maximize the light coupling to the desired micro disk optical mode before recording data. The injected light circulates hundreds or thousands of times (depending on the cavity's finesse) before exiting through the outgoing optical fiber. The output of the fiber is analyzed with a photodetector and either the transmission spectrum of the device is recorded by sweeping the laser wavelength, revealing the spectral location and spectral width of the cavity's optical modes, or modulation of the transmitted intensity as a function of the mechanical motion of the cantilever is measured by fixing the laser wavelength on the shoulder of an optical cavity mode. Motion of the cantilever results in a frequency modulation of the optical cavity modes, which can be translated into an intensity modulation by probing these modes on the side of their resonance minima. The information obtained from the transmission spectra is thus used to determine the laser wavelength for optimal transduction sensitivity. The output signal is intensity-modulated in proportion to the mechanical motion, and is transduced by a photodetector before being sent to an electronic spectrum analyzer to reveal the spectrum of mechanical modes (Fig.5). In electrical actuation experiments a network analyzer is used to measure the device transfer function – a ratio of the optical modulation to the driving force – as a function of the drive frequency.

RESULTS AND DISCUSSION

Figure 5, shows the measured thermal mechanical noise spectral density of a nitride membrane device held at four corners, similar to the one in Figure 3. A clear peak in the noise spectrum occurs at ≈ 668.1 kHz, in good agreement with a finite- element model with a nitride with tensile stress of about ≈ 150 MPa. A high mechanical quality factor of better than 110 000 is evident from the data.

A TE optical mode with an optical quality factor of ≈ 800 000 was used to carry out this measurement at a very low optical power level of approximately 3.16 µW (- 25 dBm) excitation power, 830 nW (- 30.8 dBm) at the sensor and 219 nW (- 36.6 dBm) at the photodetector, accounting for an estimated 5.8 dB fiber pigtail coupling losses at each facet. Despite the low power, the signal to noise ratio on resonance is approximately 20 dB. Low power was chosen deliberately to demonstrate the sensing performance, while also preventing the optical forces from shifting the frequency of the narrow mechanical resonance, an optical spring effect clearly observed at higher optical powers.

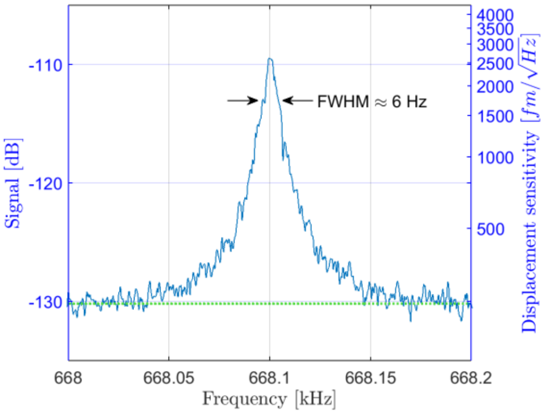


Figure 5: Measured mechanical frequency noise spectrum of the membrane transducer. The dotted green line indicates the background noise level. Signal power is reported relative to 1 mW.

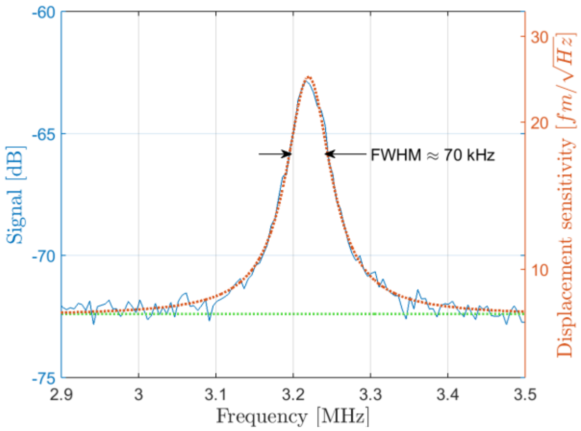


Figure 6: Measured mechanical frequency noise spectrum of the cantilever transducer with Lorentzian fit. The dotted green line indicates the background noise level. Signal power is reported relative to 1 mW.

Figure 6, shows the measured thermal mechanical noise power spectral density of a torsional cantilever transducer. The red line shows a Lorentzian fit of the power spectral density in cantilever displacement, calibrated using the equipartition method [6]. The background corresponds to the measurement noise of 9 fm/√Hz ± 0.5 fm/√Hz. The uncertainty is one standard deviation. The statistical uncertainty derived from the measurement is small. The main uncertainty is propagated form the Young's modulus used to calculate the spring constant for the displacement sensitivity calculation with the equipartition theorem. The estimated variation of the Young's modulus originating from deposition conditions is about 10 %.

We measured mechanical quality factors between ≈ 50,000 and ≈ 500 000 for the low-stress silicon nitride membrane transducers and ≈ 50 to ≈ 2 000 for the cantilever transducers which include the metallization for bimorph actuators.

Static and dynamic electrothermal actuation has been characterized. First, the static displacement of the silicon nitride structure was characterized as a function of voltage with a white light interferometer (Figure 7). The dashed red line shows a 2nd order polynomial fit to indicate the expected displacement/actuation voltage relation.

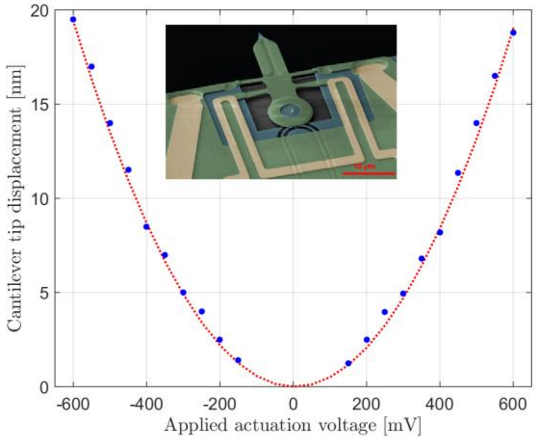


Figure 7: Relative cantilever displacement with applied DC voltage. The statistical uncertainty based on repeated measurements is smaller than the data markers.

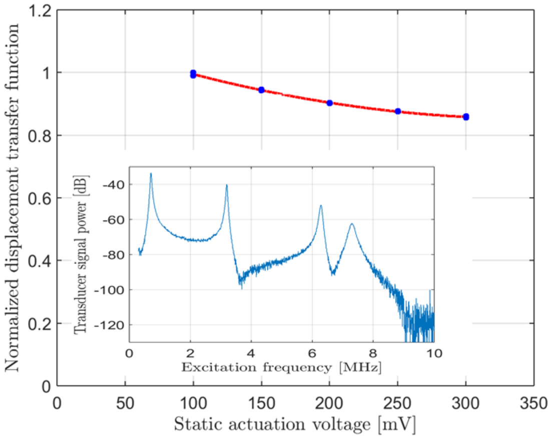


Figure 8: Normalized gain of the optomechanical displacement sensor is decreased by static actuation. The one standard deviation uncertainty based on fitting network analyzer spectrum data is smaller than the data marker size. Inset: Optomechanical signal power as a function of frequency for 8 mV AC and 50 mV DC. Signal power is reported relative to 1 mW (inset).

We then optomechanically measured the dynamic response of the structure to actuation. A small fixed modulation (AC) voltage, swept between 300 kHz and 10 MHz, was added to the actuator static bias (DC) voltage, resulting in a small, known mechanical modulation of the gap. The laser wavelength has been fixed at the steepest slope on the side of the optical resonance line at each applied DC voltage. A network analyzer was used to provide the AC voltage and detect the resulting optical power modulation, which is proportional to the motion amplitude and the optomechanical coupling. A typical optomechanically measured device transfer function is shown on the Figure 8 inset.

The AC bimorph output is proportional to the product of AC and DC voltages, as the actuation force is quadratic in applied voltage. To illustrate the tuning of the optomechanical gain by the actuator, we first normalized the displacement spectra by the DC voltage to account for the stronger drive with larger DC voltage. The resulting normalized displacement transfer function (Figure 8) reveals the gain decreasing with increasing bias as the actuator increases the transducer gap and decreases the gain of the optomechanical sensor.

The results show that the small actuation here is capable of tuning the gain by more than 10 %.

SUMMARY AND CONCLUSIONS

In summary, we have presented an overview of the design, micro- and nanofabrication, and characterization of a novel type of fully-integrated cavity optomechanical transducer platform for measurement of physical quantities by transducing them to mechanical motion. The approach of full silicon integration of all nanophotonic components with mechanically separated high-quality-factor movable components creates the opportunity to independently tailor optical, mechanical, and the actuation parts for a variety of MEMS and NEMS sensing applications that require high precision, high bandwidth, and small footprint. Additional benefits of the photonic readout approach are low power dissipation at the sensor, insensitivity to electromagnetic interference and robustness of fiber-connectorized devices. We demonstrate high mechanical and optical performance of platform components by optically detecting thermomechanical fluctuations and actuated motion of mechanical devices while tuning the optical readout gain by electrical actuation.

ACKNOWLEDGMENTS

The author would like to specially thanks Prof. Rangelow, D. Westly, and R. Ilic for helpful discussions during the development. The layout was designed with the “Nanolithography Toolbox”, a free software package developed by the Center for Nanoscale Science and Technology.

REFERENCES

[1] H. Miao, K. Srinivasan, and V. Aksyuk, “A microelectromechanically controlled cavity optomechanical sensing system,” *New J. Phys.*, vol. 14, no. 7, p. 075015, Jul. 2012.

[2] J. D. Teufel, T. Donner, M. A. Castellanos-Beltran, J. W. Harlow, and K. W. Lehnert, “Nanomechanical motion measured with an imprecision below that at the standard quantum limit,” *Nature Nanotech*, vol. 4, no. 12, pp. 820–823, Nov. 2009.

[3] T. Michels and I. W. Rangelow, “Review on Scanning Probe Micromachining and its Applications within Nanoscience,” *Vac. Sci. and Technol.*, pp. 1–21, Mar. 2014.

[4] I. Moerman, P. P. Van Daele, and P. M. Demeester, “A review on fabrication technologies for the monolithic integration of tapers with III-V smiconductor devices,” *IEEE J. Select. Topics Quantum Electron.*, vol. 6, 1997.

[5] V. R. Almeida, R. Panepucci, and M. Lipson, “Nanotaper for compact mode conversion,” *Optical Letters*, pp. 1–3, Jun. 2003.

[6] H. Li, Y. Chen, J. Noh, S. Tadesse, and M. Li, “Multichannel cavity optomechanics for all-optical amplification of radio frequency signals,” *Nature Communications*, vol. 3, pp. 1091–6, 1AD.

CONTACT
*T. Michels, tel: +1-301-975-2273; Thomas.Michels@nist.gov

The Need for Realism when Simulating Network Congestion

Kevin Mills
NIST
Gaithersburg, MD 20899
kmills@nist.gov

Chris Dabrowski
NIST
Gaithersburg, MD 20899
cdabrowski@nist.gov

ABSTRACT

Many researchers use abstract models to simulate network congestion, finding patterns that might foreshadow onset of congestion collapse. We investigate whether such abstract models yield congestion behaviors sufficiently similar to more realistic models. Beginning with an abstract model, we add elements of realism in various combinations, culminating with a high-fidelity simulation. By comparing congestion patterns among combinations, we illustrate congestion spread in abstract models differs from that in realistic models. We identify critical elements of realism needed when simulating congestion. We demonstrate a means to compare congestion patterns among simulations covering diverse configurations. We hope our contributions lead to better understanding of the need for realism when simulating network congestion.

Author Keywords

Congestion; criticality; networks; percolation; simulation

ACM Classification Keywords

I.6.1 SIMULATION AND MODELING: Model Validation and Analysis

1. INTRODUCTION

The science of complex networks [1] has matured to the point where one can study mathematical structure for many classes of probabilistic graphs (e.g., random, scale-free, small-world), as well as dynamical processes [2] moving within such graphs. Typically, abstractions are adopted in order to model real networks using techniques (e.g., graph theory and percolation theory) available from network science. Tension arises when such powerful abstractions are used to study real networks. How can one be sure that chosen abstractions adequately embody key properties of a network under study? This question of model validation motivates the work reported here.

Many researchers [e.g., 3-12] use simulation to investigate congestion spread in network topologies, often finding congestion can be modeled as a percolation process on a graph, spreading slowly under increasing load until a critical point, after which congestion spreads quickly throughout the network. The researchers identify various signals that arise around the critical point. Such signals could foreshadow onset of widespread congestion. These developments appear promising as a theoretical basis for monitoring methods that could be deployed to warn of impending congestion collapse. Despite showing promise, questions surround this research, as the models are quite abstract, bearing little resemblance to communication networks deployed based on modern technology. We explore these questions by examining the influence of realism on congestion spread in network simulations.

We begin with an abstract network simulation from the literature. We add realism elements in combinations, culminating with a high-fidelity simulation, also from the literature. By comparing patterns of congestion among the combinations, we explore a number of questions. Does spreading congestion in abstract network models mirror spreading congestion in realistic models? How do specific elements of realism influence congestion spread? What elements of realism are essential to capture in models of network congestion? What elements are unnecessary? What measures of congestion can be compared, and how, across diverse network models?

We make three main contributions. First, we illustrate congestion spread in abstract models differs significantly from spread in realistic models. Second, we identify elements of realism needed when simulating congestion. Finally, we demonstrate a method to compare congestion patterns among diverse network simulations.

The remainder of the paper is organized in five sections. Section 2 reviews some related work where researchers use abstract models to investigate congestion spread in network simulations. Section 3 describes the configurable network simulator used in our experiment. The simulator can be configured to mirror an abstract model [12], a realistic model [13], and various intermediate combinations. Section 4 details our experiment design. We present and discuss results in Sec. 5. We conclude in Sec. 6.

2. RELATED WORK

Reviewing a decade of congestion studies [3-12] reveals many similarities, and some variations, among the abstract models used. Below we summarize the models along four dimensions: topology, traffic sources/sinks, routers and

SpringSim-CNS 2016 April 3-6 Pasadena, CA, USA
© 2016 Society for Modeling & Simulation International (SCS)

Mills, Kevin; Dabrowski, Christopher.
“The Need for Realism when Simulating Network Congestion.”
Paper presented at the 19th Communications & Networking Symposium (ChinaS 2016), Pasdena, CA, Apr 3-Apr 6, 2016.

congestion measures. Elsewhere [14] we provide more details about each of the studies.

Researchers used either deterministic or probabilistic topologies. The most popular deterministic topology was a square lattice, either open [6, 11] or folded into a toroid [3-5, 7, 10]. Rykalova et al. [10] also used a ring. Echenique et al. [12] used a real topology taken from the Internet autonomous system map, circa 2001. Arrowsmith et al. [5] started with a 2D lattice and then generated triangular and hexagonal depleted lattices by probabilistically removing links. Other researchers used random processes to generate topologies: Erdős–Rényi [9], exponential [8], scale-free [8-9], or small world [9].

Within a topology, researchers used either deterministic or probabilistic processes to place sources, sinks and routers. The most popular approach was to allow every node to be a packet source and sink, as well as router [7-10, 12]. Sarkar et al. [11] restricted sources and sinks to the network edge, while Mukherjee and Manna [6] placed sources at the top edge of a lattice and sinks at the bottom edge. Other researchers [3-5] assigned nodes to be a source/sink or router with a biased coin flip. All surveyed studies generated loads by having sources inject individual packets, where each packet is destined for a randomly selected sink. The most popular strategy [3-7, 10-11] was for each source to generate a packet per time step (p/ts) with a specified probability. A few studies [8-9, 12] generated a fixed number of packets/ts and randomly assigned the packets to sources. One study [8] had a constant density option to ensure a fixed number of packets remained in transit.

In all models surveyed, router nodes queue packets arriving from sources and then forward them at an assigned rate to the next hop along some path toward the sink. Differences appeared with respect to queue discipline, next-hop selection and forwarding rate. The most popular [3-7, 9-10, 12] queue discipline was unbounded first-in, first-out (FIFO) queues. One study [8] used bounded last-in, first-out (LIFO) queues. One study [11] used bounded FIFO queues, where the oldest packet was dropped when a packet arrived at a full queue. Most studies [3-6, 10, 11] selected next hop based on shortest-path first (SPF) in hops. Ties were broken either by shortest queue length [3-4, 11], link use [5] or tossing a fair coin [6, 10]. One study [7] selected next hop with the choice among three different SPF metrics: hops, queue length, or their sum. Two studies [9, 12] used SPF based on a weighted sum of hops and queue length. One study [8] used guided random walk to select next hops. In most studies [3-5, 8, 11-12] each router forwards one p/ts. In two studies [7, 10] each router forwards one p/ts for each queue. One study [6] has each router forward a batch of packets at each time step. One study [9] assigns routers variable forwarding rates using any of three options: (1) node degree, (2) node betweeness or (3) node betweeness divided by number of nodes in the topology.

The surveyed research used various measures of network congestion, and often multiple measures per study. Congestion measures included: one-way packet latency [3-4, 6, 8]; packets delivered (i.e., aggregate throughput) [3-5]; queue lengths [4-6, 8]; packets in the network [7, 9-10, 12]; and packet drop rate [11]. Various studies analyzed the measures as time series, proportions, or variances.

Beyond the differences we identified above, the studies we surveyed shared many similarities. An abstract model is developed and then used to explore congestion in various topologies. Congestion spread is examined through selected measures. A critical load is identified, after which trajectory changes distinctly for selected measures. When examined by engineers, who deploy and manage networks based on Internet technology, the degree of abstraction is sufficiently high to call into question the findings. The topologies are rarely congruent with real Internet topologies [15], various parameter values are not consistent with real engineering choices, congestion-control protocols are not modeled and the distribution of packet injection is unlike patterns that occur with real users. Does this lack of realism matter? If so, what realism elements must be present to draw valid conclusions about congestion spread? We investigate these questions here.

3. MODELS

We conducted an experiment (see Sec. 4) with a simulation model we named FxNS (Flexible Network Simulator). FxNS is based on an abstract model, EGM, developed by Echenique, Gomez-Gardenes and Moreno [12]. We added a set of seven realism elements, factored from MesoNet [13]. While many realistic network simulators exist [16], we chose MesoNet because the model is terse (requiring only 20 parameters) and factors easily, and because the model scales (simulating up to ½ million nodes engaged in over 125×10^3 simultaneous flows).

We implemented the realism elements as options within FxNS. Since each element can be enabled or disabled, FxNS could support (2^7 =) 128 combinations. However, as explained in Sec. 3.3, we respect some dependencies among realism elements. As a result, FxNS supports only 34 combinations. FxNS can be configured to behave as EGM (most abstract model), as MesoNet (most realistic model), and any of the remaining 32 valid combinations intermediate between EGM and MesoNet. With all realism elements enabled, we use FxNS to simulate ¼ million nodes engaged in over 50×10^3 simultaneous flows. FxNS should scale up further, to the same order as MesoNet.

In Sec. 3.1 we describe EGM, and give simulation results demonstrating that FxNS correctly implements EGM. In Sec. 3.2 we describe MesoNet, and its 20 parameters spread among five categories. We also define our mapping from MesoNet parameters to FxNS realism elements. In Sec. 3.3, we justify dependencies adopted among realism elements and we describe our numbering convention for the FxNS combinations used in our experiment. Elsewhere [14] we provide additional details on these topics.

3.1. Abstract Model

In EGM, p packets are injected at each time step (ts) with source and destination nodes for each packet chosen randomly (uniform). Injected packets are placed at the end of a source's unbounded FIFO packet queue. After injection, each node can forward one packet from its queue to a next node. If the next node is the destination, the packet is delivered; otherwise the next node is chosen as the neighboring node i with minimum δ_i as defined in eq. 1:

$$\delta_i = hd_i + (1-h)c_i \tag{1}$$

where i is index of a node's neighbor, d_i is minimum hops to the packet's destination via i, and c_i is queue length of i. When h = 1 the routing amounts to SPF hops. When h < 1, routing is congestion aware, as packets may follow routes longer in hops, but shorter in total queuing delay. The lower h the more congestion-aware routing becomes.

EGM measures congestion as ρ, the ratio of packet outflow to inflow as defined in eq. 2:

$$\rho = \lim_{t\to\infty} \frac{A(t+\tau) - A(t)}{\tau p} \tag{2}$$

where A is aggregate number of packets queued, t is time, τ is measurement interval size, and p is packet-injection rate.

Using EGM with an 11 174-node topology, Echenique et al. [12] explored effects of SPF hops routing vs. congestion-aware routing as p increases. They found that for routing via SPF hops ρ undergoes a 2nd order transition as p passes a critical load, while under various degrees of congestion-aware routing ρ undergoes a 1st order transition as p passes critical load. Using our FxNS implementation of EGM, we replicated these results, as shown in Fig. 1.

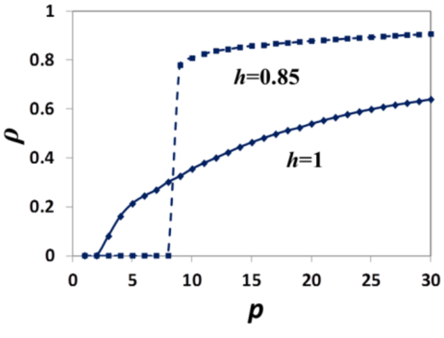


Figure 1. FxNS replication of EGM simulation results

3.2. Realistic Model

MesoNet provides a realistic TCP (Transmission Control Protocol) network model, requiring only 20 parameters spread across five categories, as shown in Table 1. Mills et al. [16] used MesoNet to compare congestion-control algorithms proposed for the Internet.

Category	ID	Name	FxNS
Network	x1	topology	NC
	x2	propagation delay	DE
	x3	network speed	VS
	x4	buffer provisioning	PD
Sources & Sinks	x5	number sources/sinks	SR
	x6	source distribution	
	x7	sink distribution	
	x8	source/sink speed	VS
Users	x9	think time	*p*
	x10	patience	n/a
	x11	web object file sizes	FL
	x12	larger file sizes	n/a
	x13	localized congestion	
	x14	long-lived flows	
Congestion Control	x15	control algorithm	TCP
	x16	initial *cwnd*	
	x17	Initial *sst*	
Simulation Control	x18	measurement interval	fixed
	x19	simulation duration	fixed
	x20	startup pattern	*p*

Table 1. MesoNet Parameters with Mapping to FxNS Elements

MesoNet allows for three-tier topologies of routers: core, point-of-presence (PoP), and access. In our experiment, we use an Internet service provider (ISP) topology shown in Fig. 2, which provides three types of access routers: D-class (red), F-class (green) and N-class. MesoNet defines speed relationships among all routers. Changing one parameter can scale network speed and higher router tiers can support the maximum input traffic expected from lower tiers. Sources and sinks can be placed below access routers as a fourth tier with ¼ million nodes (not shown in Fig. 2).

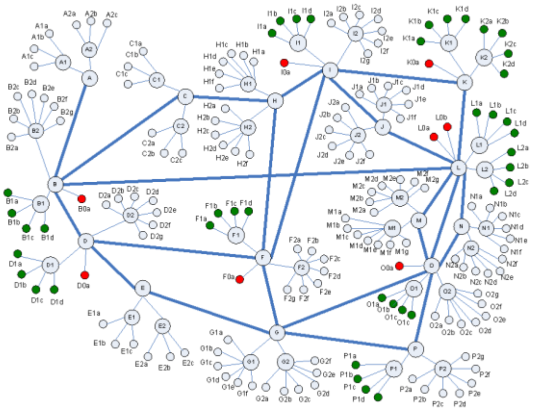


Figure 2. Three-tier 218-router topology – 16 core (A-P), 32 PoP (A1-P2) and 170 access (A1a-P2g)

FxNS maps router typing to realism element **NC** (*node classes*), which ensures that sources and sinks are placed only at the network edge. FxNS maps router speed scaling to realism element **VS** (*variable speeds*). MesoNet allows sources and sinks to connect to the network at two different speeds: fast and normal. FxNS also maps these interface speeds to realism element VS. In MesoNet links between core routers have intrinsic propagation delays matched to geographic placement and physics. FxNS maps these to realism element **DE** (*propagation delays*). These intrinsic propagation delays were used to compute SPF routes for the network core. MesoNet also includes various buffer provisioning algorithms. FxNS uses only one (estimated round-trip time multiplied by router forwarding speed) and maps this to realism element **PD** (*packet dropping*).

MesoNet allows the number of sources and sinks to be scaled and also allows probabilistic placement of sources and sinks under various types of access router. MesoNet ensures there are four times as many sinks as sources. FxNS adopts these procedures and maps them to realism element **SR** (*sources and receivers*).

MesoNet provides a rich array of user parameters, but FxNS maps only two. First, MesoNet users have think time between initiating data transfers. FxNS replaces think time with packet-injection rate, *p*. Second, MesoNet allows users to randomly select the file size for each data transfer. FxNS maps this parameter to the **FL** (*flows*) realism element, which creates sets of packets transferred in a related stream. MesoNet allows users to exhibit limited patience when waiting for data transfers to complete, but in FxNS all users have infinite patience. MesoNet allows probabilistic selection of various larger file sizes and spatiotemporal congestion. FxNS does not implement these features.

MesoNet allows probabilistic assignment of congestion-control algorithm to individual sources/sinks. In FxNS only **TCP** (*transmission control protocol*) is used. MesoNet also allows specification of initial *cwnd* (congestion window) and *sst* (slow-start threshold). FxNS maps these parameters to realism element TCP.

Finally, MesoNet offers a set of three simulation control parameters. FxNS uses measurement interval size and duration (in measurement intervals) to bound simulation length. MesoNet also allows individual traffic sources to start in a specified pattern. FxNS subsumes this under packet-injection rate.

To verify FxNS correctly implements MesoNet realism elements, we conducted comparative simulations, running MesoNet and FxNS (with all realism elements enabled) for 600 000 ts using identical parameter values. As shown elsewhere [14], we compared model output for seven essential MesoNet responses [17].

3.3. Combination Models

While FxNS can enable and disable the seven realism elements shown in Table 1, some dependencies exist, as shown in Fig. 3. Starting with all realism elements disabled (EGM), one can easily enable packet dropping (PD) and node classes (NC). Variable speeds (VS) require routers to be classified by type. Similarly, propagation delays (DE) appear on core network links, which can be identified only through router types. While sources/sinks (SR) might be included as a second tier under a flat topology, i.e., without node classes, we decided to restrict them to a fourth tier under access routers. We took this decision for convenience, allowing us to eliminate 24 combinations that would otherwise need to be simulated. We imagined influence of sources/sinks could be discerned even with this restriction. Enabling flows (FL) means packets are injected as a stream between source and sink, thus FL requires SR. Finally, TCP regulates packet-transmission rate only on flows.

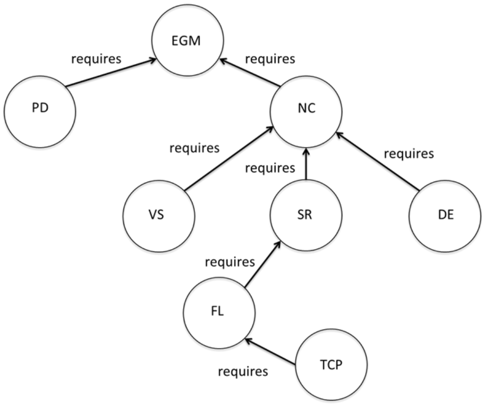


Figure 3. Dependencies among FxNS realism elements

Seq	Cmb	TCP	FL	SR	DE	VS	NC	PD
1	c0	0	0	0	0	0	0	0
2	c1	0	0	0	0	0	0	1
3	c2	0	0	0	0	0	1	0
• • •								
32	c123	1	1	1	1	0	1	1
33	c126	1	1	1	1	1	1	0
34	c127	1	1	1	1	1	1	1

Table 2. Elided list of valid FxNS combinations

We identify FxNS combinations by number, based on binary encoding, as shown in Table 2. Each realism element is assigned a position in a seven-bit vector, from most (bit 7 - TCP) to least (bit 1 - PD) significant. When a selected factor is enabled its bit position is set to one, and set to zero when disabled. The resultant bit vector can be converted to a decimal value: the combination (Cmb) number. The most abstract combination is c0 and the most realistic is c127. Each combination is also assigned a sequence (Seq) number (1-34). Both numbers are used in discussing results.

4. EXPERIMENT DESIGN

We designed an experiment to explore influence of realism on congestion spread in a network simulated with FxNS. We identify fixed input parameters used in all simulations. We define parameters we vary. We define four responses measured for all simulations.

4.1. Fixed Input Parameters

We used the same 218-router topology (recall Fig. 2) in all simulations. We used Dijkstra's SPF algorithm to compute next hops for core routers based on propagation delays. Routing to/from core nodes consists of single paths with obvious next hops. Note that propagation delays are used to compute SPF next hops in the core regardless of whether DE is enabled or disabled.

We execute each simulation for a target of 200 000 ts. Individual simulations can self-adapt to execute fewer ts in order to limit memory usage when PD is disabled. No simulation executed fewer than 41 400 ts.

4.2. Variable Input Parameters

We varied only two parameters: (1) combination and (2) packet-injection rate *p*. For each combination, FxNS simulates a set of enabled/disabled realism elements (recall Table 2). Table 3 gives parameter values assigned to each element when enabled and disabled.

For each combination simulated, we varied *p* up to 2500. When extreme congestion appears at successive values of *p*, simulation of a combination could self-terminate. This saves computation time because once a combination demonstrates extreme congestion for several increasing values of *p* then the combination will continue to exhibit congestion as *p* increases. In no case did a simulation terminate a combination before *p* passed 790.

4.3. Responses

We chose responses that could be usefully compared across all simulated combinations: most abstract to realistic. We determined that all combinations shared two measurable concepts: graphs and packets. Using these we measure: congestion spread (χ), network connectivity (α) and effectiveness (π) and efficiency (δ) of packet delivery. All responses fall in the interval [0...1]. We measure each response for each combination at each packet-injection rate. We define these responses precisely elsewhere [14]. Here we give intuitive definitions.

Each of our simulated topologies is a graph of nodes connected by links, where the entire graph G_N contains $|G_N|$ nodes. We label a node congested whenever queued packets exceed 70 % of 250×router forwarding speed. When fewer packets are queued, we label a node uncongested. We label any uncongested node as cutoff when it links only to congested neighbors. After labeling, we compute connected subgraphs of nodes that are either congested or cutoff. We label the largest such subgraph G_χ. We use $\chi=|G_\chi|/|G_N|$ as a measure of congestion spread. We also compute connected subgraphs of nodes that are uncongested. We label the largest such subgraph G_α. We use $\alpha=|G_\alpha|/|G_N|$ as a measure of network connectivity.

	Enabled	Disabled
PD	buffers = 250×router speed	buffers = ∞
NC	3-tier 218-node topology as in Fig. 2 with routers labeled as core, PoP, D-class, F-class or N-class	flat 218-node topology as in Fig. 2 but with routers unlabeled
VS	core 80 p/ts; PoP 10 p/ts; D-class 10 p/ts; F-class 2 p/ts; N-class 1 p/ts; fast source/sink 2 p/ts; normal source/sink 0.2 p/ts	all routers and sources/sinks 9 p/ts
DE	core links have propagation delays	no propagation delays
SR	51 588 sources & 206 352 sinks deployed uniformly below access routers	no sources or sinks deployed
FL	transfers are packet streams: sized randomly from Pareto distribution (mean 350, shape 1.5) - streams set up with TCP connection procedures	transfers are individual packets
TCP	packet transmission regulated by TCP congestion-control including slow-start (initial *cwnd* = 2 *sst* = $2^{30}/2$) and congestion avoidance	packet transmissions not regulated by congestion-control

Table 3. Parameter values for each FxNS realism element

Packets injected into the network can be queued, dropped or delivered. We define effectiveness of packet delivery (π) as the ratio of delivered packets to injected packets. For each delivered packet we record the latency between injection and delivery times. We average these latencies over all delivered packets, and then normalize the average to fall between 0 (minimum delay) and 1 (maximum delay), yielding efficiency (δ) of packet delivery.

5. RESULTS AND DISCUSSION

For each combination simulated, we plotted each response (*y*-axis) vs. packet-injection rate (*x*-axis). Here we give plots for only the most abstract (c0) and realistic (c127) combinations, as discussed in Sec. 5.1. For each response, we also treat each of the 34 plots, one for each combination, as a 250-element vector and then cluster vectors to assess influence of each realism element on each response. We discuss the clusters in Secs. 5.2 to 5.5, drawing on insights from the related *x*-*y* plots and multidimensional interactive visualization of FxNS simulation data [18]. All *x*-*y* and cluster plots are also available in an enlarged format [19].

5.1. Most Abstract vs. Most Realistic

Figure 4 contains four subplots comparing congestion behavior between the most abstract (c0) and realistic (c127) combinations. For combination c0, congestion spreads quickly with increasing packet-injection rate, encompassing all nodes by the time *p* reaches 500. For c127, congestion spread remains low over the entire range of packet-injection rates, even out to *p* = 2500 (not shown). This difference has two main causes. First, all nodes in c0 operate at the same speed. Core nodes become overwhelmed with congestion, which then spreads to the network edge. In c127, routers are engineered with varying, hierarchical speeds, so higher tiers can handle packet inflow rate from lower tiers. Second, c0 does not monitor and adapt to congestion, while c127 implements TCP, which measures congestion and adapts packet inflow-rate accordingly.

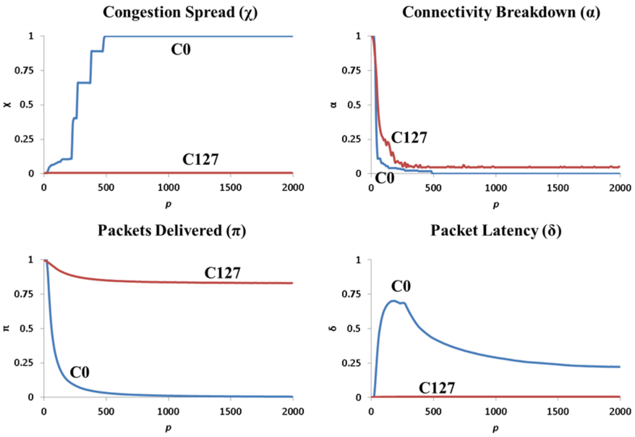


Figure 4. Comparing c0 vs. c127 for each response

Network connectivity breaks down quickly for both c0 and c127, reaching a low level as *p* passes 500. There are two main differences: c127 decays more slowly than c0 and c127 asymptotes with higher network connectivity. For c0 connectivity drops to zero after *p* passes 500. Combination c127 decays more slowly because TCP adapts packet injection based on measured congestion and c127 asymptotes with higher connectivity because variable router speeds restrict congestion to the network edge. The network core remains uncongested and intact. Connectivity breaks down completely for c0 because the core becomes congested and then congestion spreads to the edge, consuming all nodes.

For c0 proportion of packets delivered drops steeply, reaching nearly zero as *p* passes 1000. For c127 proportion of packets delivered drops modestly with increasing *p*, stabilizing near 80 %. This large difference arises from a combination of two factors: packet dropping and TCP. Combination c0 does not discard packets and does not adapt packet injection based on measured congestion. With increasing *p*, this causes a growing backlog of packets in all routers. Combination c127 discards packets when router buffers fill and adapts packet injection based on measured congestion. So undelivered packets for c127 encompass only discards, and rate adaptation limits their number.

For c127 latency of delivered packets remains low even as *p* increases beyond 2000. This occurs because packet dropping limits router queue sizes, so delivered packets are not long delayed. Without packet dropping, packet latency for c0 climbs steeply with increasing *p*, reaching an apex before decaying gradually. Delays climb because packet queues become jammed. Delays decay gradually because latencies are recorded only for delivered packets. At high *p*, c0 delivers relatively few packets, and those packets necessarily transit routes where queues are not jammed. Even with this decay, packet latency for c0 remains significantly above delay for c127.

5.2. Congestion Spread

Figure 5 shows hierarchical clustering for χ among all 34 combinations. Combination sequence numbers appear on the *x*-axis. The *y*-axis reports squared Euclidean distance. The plot indicates two main groups, separated by a large distance. The left-hand group contains combinations with VS or TCP or both enabled. These combinations show little congestion spread. Combinations in the right-hand group have VS and TCP disabled. These combinations show congestion spreading throughout the network.

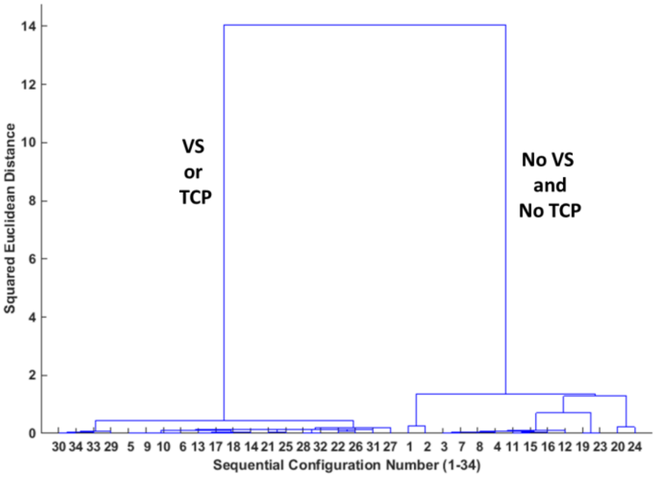


Figure 5. Clustering of congestion spread (χ)

5.3. Connectivity Breakdown

Figure 6 shows clustering for α. Note that distances among clusters in Fig. 6 are smaller than those in Fig. 5. This means connectivity breakdown is more similar among the combinations than is congestion spread. Breakdown in connectivity occurs when subgraphs of the topology are disconnected (due to congestion). As load increases connectivity breaks down even when congestion does not necessarily spread widely. Among combinations with VS disabled, the leftmost subgroup (sequence numbers 12, 15, 11, 3, 7, 8 and 16) in Fig. 6 has NC enabled. Our *x-y* plots show [19] these combinations reach complete breakdown sooner than others with VS disabled. With NC enabled, packet injection occurs at the network edge, thus packets flow in concentrated fashion to and through the network core. This differs from combinations c0 and c1 (sequence numbers 1 and 2), where packet injection can occur at any node, thus packet flow is more diffuse. Most configurations with VS disabled lost connectivity quickly and completely. Combinations with VS enabled and TCP disabled may experience complete connectivity breakdown, but the process requires higher packet-injection rates because more pressure must be applied from the edge before the core can congest. With both TCP and VS enabled, congestion stays at the edge.

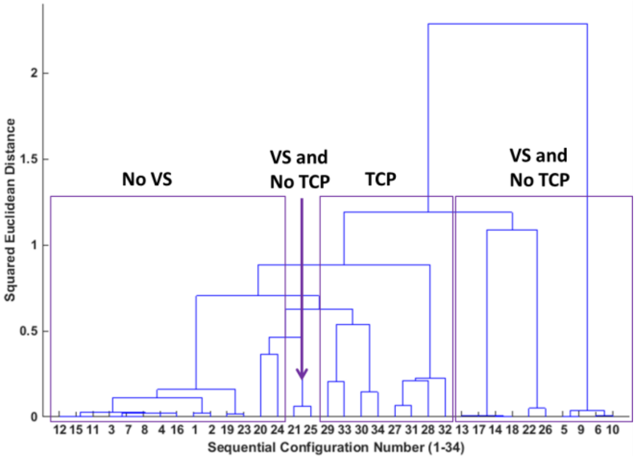


Figure 6. Clustering of breakdown in connectivity (**α**)

5.4. Packets Delivered

Figure 7 shows clustering for π. The plot indicates two main groups, separated by a large distance. The leftmost group contains combinations with TCP disabled, while the rightmost contains combinations with TCP enabled. The rate adaptation of TCP improves significantly the likelihood that an injected packet will reach the intended destination. Disabling TCP increases likelihood that an injected packet will be queued or discarded.

With TCP enabled, PD has a secondary influence on packet delivery. Disabling PD ensures that injected packets will be delivered eventually. But buildup of queues delays delivery, leading to timeouts and lower throughputs, as TCP reduces packet-injection rate. Enabling PD means some packets will be discarded, but TCP does not need to reduce injection rate as much. So throughputs remain higher, but likelihood of packet delivery decreases.

With TCP disabled, VS has secondary influence on packet delivery. Absence of VS allows queues to build widely among routers throughout a network. So, packets are more likely to be queued or discarded (depending on PD), and packet delivery approaches zero. With VS enabled packet queues build at the network edge. This reduces the number of routers where packets will be dropped or queued. In such cases, packet delivery approaches zero at a slower rate.

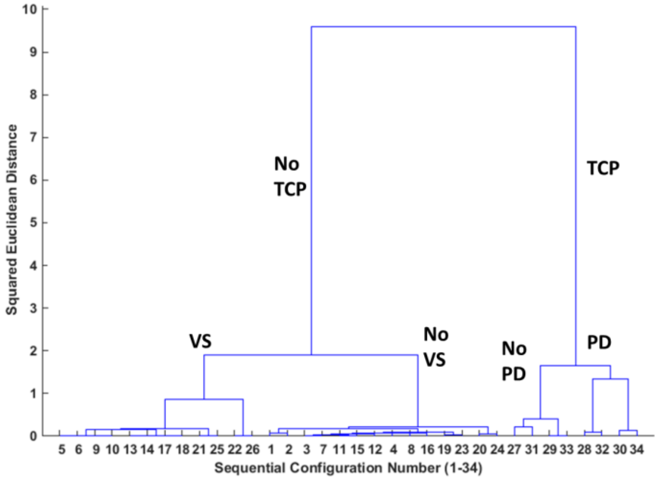


Figure 7. Clustering of packet delivery effectiveness (**π**)

5.5. Packet Latency

Figure 8 shows clustering for δ. We label the plot to show common factors in various groups and subgroups. With PD enabled, delivered packets experience little queuing delay, thus one-way latency is low. With PD disabled, packet queues become large with load, thus average one-way latency increases. With PD disabled, enabling TCP allows rate adaptation, thus buildup of large queues is less likely. This reduces delays for delivered packets. Enabling VS restricts large queues to routers at the network edge, which means that delivered packets have fewer large queues to transit. Disabling VS allows packet queues to form at any network router, which means delivered packets will have to transit through more large queues.

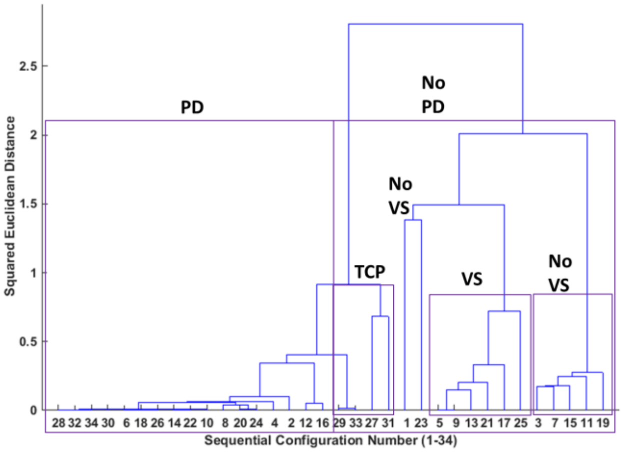


Figure 8. Clustering of packet delivery efficiency (δ)

5.6. Overall Findings

Realistic and abstract network models exhibit very different congestion behaviors. VS among router tiers, engineered to ensure adequate throughput, are very important to model. TCP, which detects congestion and adapts packet-injection rate, is very important to model. PD from finite FIFO buffers is important to model for accurate measures of packet latency. Propagation delay (DE) is not important to model in networks spanning the continental US, but would be important in networks (e.g., interplanetary) where propagation delays may exceed queuing delays. A decade of studies [e.g., 3-12] used models too abstract to simulate realistic congestion in networks based on Internet technology. The validity of findings from such studies appears suspect.

6. CONCLUSION

We began with an abstract network simulation from the literature. We added realism elements in combinations, culminating with a high-fidelity simulation, also from the literature. By comparing patterns of congestion among the combinations, we showed that congestion spread in abstract models differs from congestion spread in realistic models. We described the influence of specific realism elements on congestion spread. We found that variable router speeds, the transmission-control protocol, and finite first-in, first-out buffers are important to model. We also found that propagation delay appears unimportant to model, when a simulated topology spans only the US. Finally, we demonstrated use of cluster analyses among response vectors to compare congestion spread, breakdown in connectivity and effectiveness and efficiency of packet delivery among a diverse set of network models.

We envision two directions for future work. First, we need to verify our findings for a variety of topologies, including interconnected networks. Second, we should explore whether random failures in the core, coupled with alternate routing, could cause cascading congestion. If so, we can seek precursor signals arising around the critical point. Such signals, if found, might provide warning of failure-induced congestion collapse.

ACKNOWLEDGMENTS

We appreciate financial support and encouragement by our laboratory management. We benefited from the review of our colleagues Guo Yang, Phil Gough, and Sandy Ressler, and also from anonymous, external reviewers.

REFERENCES

1. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M. and Hwang, D.-U. Complex networks: structure and dynamics, *Physics Reports*, 424 (2006), 175-308.
2. Stauffer, D. and Aharony, A. *Introduction to percolation theory: revised second edition*. Taylor & Francis, 1994.
3. Solé, R. and Valverde, S. Information transfer and phase transitions in a model of internet traffic, *Physica A*, 289 (2001), 595-605.
4. Woolf, M., Arrowsmith, D., Mondragon, R. and Pitts, J. Optimization and phase transitions in a chaotic model of data traffic, *Phys Rev E*, 66 (2002), 046106.
5. Arrowsmith, D., Mondragon, R., Pitts, J. and Woolf, M. Phase transitions in packet traffic on regular networks, ISSN 1103-467X, Institut Mittag-Leffler, 2004.
6. Mukherjee, G. and Manna, S. Phase transition in a directed traffic flow network, *Phys Rev E*, 71, 6 (2005), 066108.
7. Lawniczak, A., Lio, P., Xie, S. and Xu, J. Study of packet traffic fluctuations near phase transition point from free flow to congestion in data network model, in *Canadian Conference on Electrical and Computer Engineering*, (2007), 360-363.
8. Tadic, B., Rodgers, G. and Thurner, S. Transport on complex networks: flow, jamming and optimization, *International Journal of Bifurcation and Chaos*, 17, 7, (2007), 2363-2385.
9. Wang, D., Cai, N., Jing, Y. and Zhang, S. Phase transition in complex networks, *American Control Conference*, (2009), 3310-3313.
10. Rykalova, Y., Levitin, L. and Brower, R. Critical phenomena in discrete-time interconnection networks, *Physica A*, 389 (2010), 5259-5278.
11. Sarkar, S., Mukherjee, K., Ray, A., Srivastav, A. and Wettergren, T. Statistical mechanics-inspired modeling of heterogeneous packet transmission in communication networks, *IEEE Trans on Syst, Man, and Cybernetics—Part B: Cybernetics*, 42, 4 (2012), 1083-1094.
12. Echenique, P., Gomez-Gardenes, J. and Moreno, Y. Dynamics of jamming transitions in complex networks, *Europhys Lett*, 71, 2 (2005), 325.
13. Mills, K., Schwartz, E. and Yuan, J. How to model a TCP/IP network using only 20 parameters, *Winter Simulation Conference*, (2010), 849-860.
14. Dabrowski, C. and Mills, K. *The Influence of Realism on Congestion in Network Simulations*, NIST Technical Note 1905, January 2016, 62 pages. doi:10.6028/NIST.TN.1905. As of 5 Feb 2016.
15. Doyle, J., Alderson, D., Li, L., Low, S., Rougan, M., Shalunov, S., Tanaka, R. and Willinger, W. The “robust yet fragile” nature of the internet, *National Academy of Sciences*, 102, 41 (2005), 14497-14502.
16. Mills, K., Filliben, J., Cho, D., Schwartz, E. and Genin, D. *Study of proposed internet congestion control algorithms*, NIST SP 500-282, 2010.
17. Mills, K. and Filliben, J. Comparison of two dimension-reduction methods for network simulation models, *Journal of Research of the National Institute of Standards and Technology*, 116**,** 5 (2011), 771-783.
18. Gough, P., Multidimensional Interactive Visualization of FxNS Simulation Data. http://tinyurl.com/payglq6. As of 22 Oct 2015.
19. Dabrowski, C. and Mills, K. FxNS graphs enlarged. http://tinyurl.com/poylful. As of 15 Oct 2015.

Vulnerabilities of "McEliece in the World of Escher"

Dustin Moody[1] and Ray Perlner[1]

[1]National Institute of Standards and Technology,
Gaithersburg, Maryland, USA

dustin.moody@nist.gov, ray.perlner@nist.gov

Abstract. Recently, Gligoroski et al. proposed code-based encryption and signature schemes using list decoding, blockwise triangular private keys, and a nonuniform error pattern based on "generalized error sets." The general approach was referred to as *McEliece in the World of Escher.* This paper demonstrates attacks which are significantly cheaper than the claimed security level of the parameters given by Gligoroski et al. We implemented an attack on the proposed 80-bit parameters which was able to recover private keys for both encryption and signatures in approximately 2 hours on a single laptop. We further find that increasing the parameters to avoid our attack will require parameters to grow by (at least) two orders of magnitude for encryption, and may not be achievable at all for signatures.

Keywords: Information Set Decoding, Code-based Cryptography, McEliece PKC, McEliece in the World of Escher

1 Introduction

The McEliece cryptosystem [1] is one of the oldest and most studied candidates for a postquantum cryptosystem. McEliece's original scheme used Goppa codes, but other families of codes have been proposed, such as moderate density parity check codes [2] and low rank parity check codes [3, 4]. Recently, Gligoroski et al. [5, 6] proposed a new approach to designing a code-based cryptosystem. Their approach uses a blockwise-triangular private key to enable decryption and signatures through a list decoding algorithm. The error vector in both cases is characterized, not by a maximum Hamming weight t, as is typical for code-based cryptosystems, but by an alphabet of allowed ℓ-bit substrings known as the *generalized error set.* Claimed advantages of this approach include a straightforward signature scheme and the ability to analyze security by using the tools of algebraic cryptanalysis.

The concept of information set decoding originates with Prange [7]. Further optimizations were subsequently proposed by Lee and Brickell [8], Leon [9], Stern [10], and several others [11–14]. Information set decoding techniques can be used to attack code-based cryptosystems in several ways. They can be used to search for a low-weight error vector directly, or they can be used to detect

Disclaimer: Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

Moody, Dustin; Perlner, Ray.
"Vulnerabilities of "McEliece in the World of Escher"."
Paper presented at the 7th International Workshop on Post-Quantum Cryptography, Fukuoka, Japan, Feb 24-Feb 26, 2016.

hidden structure in the public generator or parity check matrices by finding low weight code words in the row space of the generator matrix or parity check matrix. All of these applications of information set decoding are relevant to the scheme of Gligoroski et al. We will refer to their scheme as *McEliece Escher*, since it was introduced in their paper *McEliece in the World of Escher* [5, 6]. We demonstrate that information set decoding techniques are much more effective against the McEliece Escher scheme than suggested by the authors' original security analysis.

Gligoroski et al. were aware of both categories of information set decoding attacks on their scheme, but their analysis of these attacks was incomplete. Most seriously, they believed that information set decoding only produced a distinguisher on the private key, rather than a full key recovery, and they failed to consider the application of information set decoding to find a valid error vector in the signature setting. Landais and Tillich [15] applied similar techniques to convolutional codes, which have similar structure to the private keys used by McEliece Escher. We offer improvements to the existing approaches, including showing how to take advantage of the structured permutation used by McEliece Escher to disguise the private generator matrix.

Furthermore, we show our attacks are practical. Using the proposed parameters for 80-bits of security, we were able to recover private keys for both encryption and signatures in less than 2 hours on a single laptop. We find that increasing the parameters to avoid our attack will require parameters to grow by (at least) two orders of magnitude for encryption, and may not be practical at all for signature.

2 Background: McEliece schemes

2.1 Public and Private Keys

Gligoroski et al. construct their scheme along the lines of the original McEliece cryptosystem. The public key is a $k \times n$ generator matrix G_{pub} for a linear code over $\mathbb{F}_2$. To encrypt a message, the sender encodes a k-bit message m as an n bit codeword and then intentionally introduces errors by adding an error vector e. The ciphertext is then given by:

$$c = mG_{pub} + e.$$

Gligoroski et al. also introduce a signature scheme by applying the decoding algorithm to a hashed message. A signature σ is verified by checking

$$\mathcal{H}(m) = \sigma G_{pub} + e,$$

for a suitably chosen hash function $\mathcal{H}$.

Similar to the ordinary McEliece scheme, G_{pub} is constructed from a structured private generator matrix G, an arbitrary $k \times k$ invertible matrix S, and an $n \times n$ permutation matrix P.

$$G_{pub} = SGP. \tag{1}$$

For encryption, G_{pub} must be chosen in such a way that the private key allows unique decoding of a properly constructed ciphertext. For signatures, on the other hand, G_{pub} must be constructed to allow some decoding (not necessarily unique) of a randomly chosen message digest.

It will sometimes be helpful to characterize the public and private codes by their parity check matrices. The private parity check matrix, H is a $(n-k) \times n$ matrix, related to the private generator matrix G by the relation

$$GH^T = 0.$$

Similarly, it is easy to construct a public parity check matrix H_{pub} from G_{pub}, characterized by the relation $G_{pub}H_{pub}^T = 0$. This will be related to the private parity check matrix as

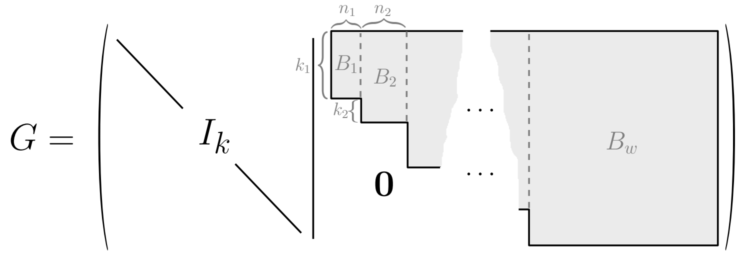
$$H_{pub} = S'HP,$$

where S' is an $(n-k)\times(n-k)$ invertible matrix and P is the same permutation matrix as in Equation (1).

2.2 Private Generator and Parity Check Matrices

To construct the binary (n, k) code used in the McEliece Escher scheme, the (private) generator matrix is of the form illustrated in Figure 1. Each block B_i is a random binary matrix of dimension $(\sum_{j=1}^{i} k_j) \times n_i$, so that $k = k_1 + k_2 + \cdots + k_w$ and $n = k + n_1 + n_2 + \cdots + n_w$. The corresponding private parity check matrix is depicted in Figure 2, and has a similar block-wise structure. For ease of notation, we will let $K = (k_1, k_2, .., k_w)$ and $N = (n_1, n_2, .., n_w)$.

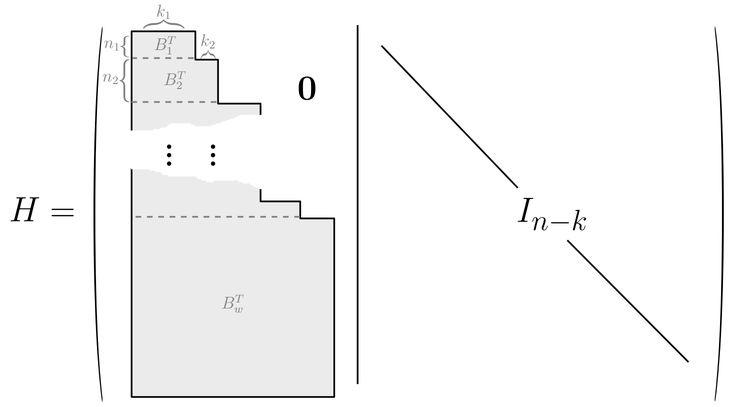
Fig. 1. The private generator matrix



2.3 Error Sets

In the McEliece Escher scheme, the error vector is broken up into n/ℓ segments, each ℓ-bits. The value ℓ is called the *granularity* of the scheme, and for all proposed parameter sets, ℓ is set to 2. While the original McEliece scheme restricted the error vectors to having a low Hamming weight t, the McEliece

Fig. 2. The private parity check matrix



Escher scheme instead restricts the error space by choosing each ℓ-bit subsegment from a limited alphabet, called an *error set*. Error sets may be analyzed in terms of a density parameter ρ given by the formula

$$\rho = |E|^{1/\ell}.$$

For the proposed parameters, the error set is always $E = \{00, 01, 10\}$. This error set has granularity $\ell = 2$ and density $\rho = \sqrt{3}$.

Since public key operations require the encrypter or verifier to distinguish between valid and invalid error vectors, the permutation P used to disguise the private generator and parity check matrices must necessarily be of a special form. The action of P needs to rearrange ℓ-bit segments of the rows, but leave the segments themselves intact. In other words, P must consist of $\ell \times \ell$ blocks which are either 0 or the identity matrix I_ℓ.

3 Improving Information Set Decoding for the Error Vector

Information set decoding may be used to recover m and e from the ciphertext $c = mG_{pub} + e$. The basic strategy involves guessing k bits of the error vector and recovering the rest by linear algebra. One of the simplest information set decoding algorithms is given in Algorithm 1.

It should be clear that the number of iterations this algorithm requires is inversely proportional to the probability that an attacker can guess k bits of the error vector. As in the case of standard McEliece, the most probable guess for these k bits is the all zero vector. However, since McEliece Escher uses a nonuniform error pattern, the choice of the permutation P' has a significant effect on the probability of success. In their security analysis, Gligoroski et al. assumed that P' would be of similar form to the secret permutation matrix P used to disguise the private key. This has the effect of forcing the adversary to guess all the bits in each ℓ-bit block chosen from a generalized error

```
Algorithm 1: Information set decoding for the error vector
Input: ciphertext $c$, and a parameter $k$
Output: message $m$, error $e$
  1. Permute the bits of the ciphertext by a random permutation matrix $P'$:
         $c' = (mG_{pub} + e)P'$
         $\quad = mG_{pub}P' + eP'$
         $\quad = m(A|B) + (e'_1|e'_2)$
         $\quad = (mA + e'_1)|(mB + e'_2),$
     where $A$ and $e'_1$ are the first $k$ columns of the permuted generator matrix $G_{pub}P'$
     and permuted error vector $eP'$, respectively.
  2. If $A$ is not invertible, go to step 1.
  3. Guess $e'_1$. If correct the message can be reconstructed as
         $m = ((mA + e'_1) - e'_1)A^{-1}.$
     The error vector is then $e = c - mG_{pub}$.
  4. If the error vector is properly formed (i.e., the Hamming weight is less than $t$ for
     standard McEliece, or composed of $\ell$-bit substrings from the proper generalized
     error set in McEliece Escher), return $m$ and $e$. Otherwise go back to step 1 and start
     over with a new permutation $P'$.
```

set. Thus the probability of each guess is ρ^{-k}. However, an attacker can do better by choosing a permutation that always separates the bits of an ℓ-bit block. For example, each bit is 0 two-thirds of the time when the error set is $E = \{00, 01, 10\}$, but both bits are 0 only one-third of the time. By guessing one bit within each 2-bit block, an attacker achieves a success probability of $(2/3)^k$, which is a significant improvement over the value $(1/\sqrt{3})^k$ assumed by Gligoroski et al.'s security analysis. Concretely, when used against Gligoroski et al.'s claimed 80-bit secure code with parameters $(n, k) = (1160, 160)$, the probability of a single guess of k bits of the error vector improves from 2^{-127} to 2^{-94}.

Similar improvements are available for more sophisticated decoding algorithms. In section 5.1 of their paper [5], Gligoroski et al analyze modifications to several information set decoding algorithms [8, 10–14], including several that use meet-in-the-middle strategies to try several guesses at once, and apply them to the case where $k = 256$. For our purposes these algorithms may be characterized by the number of bits $k+\lambda$ which are guessed, along with the Hamming weight p of those guesses. Whenever $p \cdot \log_2(\sqrt{3}) < (k + \lambda)\log_2(\frac{2}{\sqrt{3}})$, the modification described above decreases the complexity of decoding by a factor of at least $2^{(k+\lambda)\log_2(\frac{2}{\sqrt{3}}) - p\cdot\log_2(\sqrt{3})}$. This is true for some of the algorithms analyzed by Gligoroski et al. For example, Stern's algorithm is quoted as having a complexity of 2^{197} when applied to $k = 256$, however, with our modification, Stern's algorithm with $p = 2$ has a probability of success per iteration of approximately 2^{-136} corresponding to a complexity somewhere around 2^{150}. It does not however appear that a direct application of our modification improves the most efficient algorithm analyzed by Gligoroski et al., since p is apparently too large. This algorithm, adapted from the BJMM algorithm [14], is quoted as achieving a complexity of 2^{123}. It is possible that some sort of hybrid approach will provide an improvement. Nonetheless, for the remainder of this paper, we will assume that Gligoroski et al.'s analysis of the complexity of attacking the encryption algorithm, by direct search for a unique patterned error vector, is correct.

Algorithm 1, modified so that as many ℓ-bit blocks as possible of the error are spit between e_1' and e_2', is however an extremely effective method for signature forgery. For the error set $E = \{00, 01, 10\}$, when a 2-bit block is split between e_1' and e_2', the bit in e_1' may be forced to 0, and the pair of bits will remain within the error set, whether the corresponding bit in e_2' is set to 0 or 1. If all the bits of e_1' are set to 0, then the probability for the resultant error vector e to be a valid error vector is $(\frac{\sqrt{3}}{2})^{n-2k}$. For the claimed 80-bit secure signature code with parameters $(n, k) = (650, 306)$, this probability is approximately 2^{-8}.

4 Information Set Decoding for the Private Key

Information set decoding techniques can also be used to find low weight elements in the row spaces of matrices. In our case, we are interested in the public generator and parity check matrices, G_{pub} and H_{pub}. Note that elements of these public row spaces are related to the elements of the row spaces of the private generator and parity check matrices by the permutation P used in the construction of the public key:

$$vG_{pub} = ((vS)G)P,$$

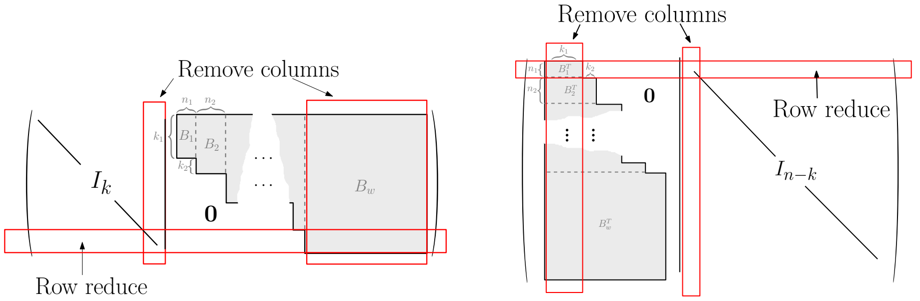
$$v'H_{pub} = ((v'S')H)P,$$

where v and v' are k and $(n-k)$-bit row vectors respectively. Consequently, the result of an information set decoding attack on G_{pub} or H_{pub} will simply be the image under P of a low weight element of the row space of G or H. We thus examine the space of low weight vectors for encryption and signatures.

Recall the description of the private generator and parity check matrices given in Section 2.2. For encryption, the private key operation requires maintaining a list of at least ρ^{k_1} entries. This means that k_1 must be small in order for the scheme to be efficient. The first n_1 rows of H are forced by construction to have nonzero bits only in the $(n_1 + k_1)$ columns $C_j(H)$, with $1 \leq j \leq k_1$ or $k + 1 \leq j \leq k + n_1$. Linear combinations of these rows will then produce approximately $\binom{n_1+k_1}{t}2^{-k_1}$ distinct row vectors of weight t. The general attack strategy will be to seek to sample from the images under P of this space of low weight row vectors, which are constrained to only contain nonzero bits in columns C_j, with the same bounds on j as above. We thereby learn the images of those columns, and once learned they can be removed from H_{pub}. The row space of the matrix formed by the remaining columns of H is the same as for the parity check matrix of a code of the same structure with $w' = w - 1$, $N' = (n_2, .., n_w)$, $K' = (k_2, .., k_w)$. Applying this strategy recursively will allow us to identify the underlying block structure and construct a new private key of the same form.

For signatures, the private key operation requires maintaining a list of at least $(2/\rho)^{n_w}$ entries. In order for the scheme to be efficient, n_w must be small. The last k_w rows of G have zero bits everywhere, except possibly in the (k_w+n_w) columns $C_j(G)$, indexed by $(k-k_w+1) \leq j \leq k$ and $(n-n_w+1) \leq j \leq n$. Linear combinations of the rows will produce approximately $\binom{k_w+n_w}{t} 2^{-n_w}$ distinct row vectors of weight t. Similarly as done for encryption, the strategy for signatures will be to seek to sample from the images under P of this space of low weight row vectors, learning the images of the aforementioned columns. Once the columns have been learned, they can be removed from G_{pub} and the process recursively repeated since the row space of the matrix formed by the remaining columns of G is that of a parity check matrix for a code of the same form with $w' = w-1$, $N' = (n_1, .., n_{w-1})$, $K' = (k_1, .., k_{w-1})$. See Figure 3 for an illustration of the strategy for both encryption and signatures.

Fig. 3. Removing columns and row-reducing leaves a smaller code of the same form.



It should be noted that the space of short vectors with support on the target columns is not the only source of low weight vectors that can be obtained by information set decoding algorithms. However, for realistic parameters, it is generally advantageous to simply choose t to maximize the rate at which vectors from the target space are produced. This is because there is an efficient way to use a list of vectors, some of which are from the target space and some of which are not, to produce a full list of the target columns. The algorithm that does this uses a subroutine which is applied to a small subset of the list of vectors, and which will usually produce the full list of target columns if the chosen vectors are all from the target space. This subroutine will not only terminate quickly on correct inputs, but also if one of the vectors is not from the target space. In the latter case the algorithm will recognizably fail, by identifying too many columns. The first obtained list of vectors, required to recover the full target set of columns, will generally be small enough that trying the subroutine on all appropriately sized subsets of the list will be of insignificant cost compared to the information set decoding steps.

The subroutine proceeds as follows (see Alg. 2). The input is a list of target columns, containing at least $(k_1 + 1)$ of the target columns for encryption (or at least $(n_w + 1)$ of the target columns for signatures). These columns may generally be obtained by combining the nonzero positions of a small number (e.g. two) of the target vectors produced by an information set decoding algorithm, such as Stern's algorithm.

Algorithm 2: Subroutine to complete the list of target columns

```
Input: A set $S$ of columns
Output: A set of columns S' ⊇ S, and a flag "Success" or "Failure"
  1. Check whether removing the columns of $S$ from the public matrix reduces the rank.
       – If all of the columns are from the target set, then removing the columns in $S$ will
         likely reduce the rank of the public matrix by $|S| - k_1$ for encryption (or $|S| - n_w$
         for signatures).
  2. For each column $C$ not in $S$, check whether the rank of the public matrix is
     decreased when $C$ is removed in addition to those already in $S$.
     (a) if the rank is decreased, add $C$ to $S$ and repeat step 2.
     (b) if the rank stays the same for each $C \notin S$, return $S' = S$ and go to the last step to
         determine success.
  3. The algorithm succeeds if the rank stops decreasing at $n - k - n_1$ for encryption (or
     $k - k_w$ for signatures). Otherwise output failure.
```

4.1 Using the Nonrandom P

The attack outlined in the previous section does not take into account the constraints on the permutation P used to disguise the private key G (or H). In particular, the permutation leaves blocks of ℓ consecutive columns intact. Thus, there is additional information about the location of our target columns that we did not use. In particular, if the column C_j is in our target set, we can be confident that all the columns $C_{\lfloor \frac{j-1}{\ell} \rfloor+1}, ..., C_{\lfloor \frac{j-1}{\ell} \rfloor+\ell}$ are also in the target set. We modify Stern's algorithm to take advantage of this by choosing our random permutation P' in such a way as to leave ℓ-bit blocks of columns intact, just as the private matrix P does. We will also count the number of nonzero ℓ-bit blocks within a row vector as a substitute for Hamming weight, wherever Hamming weight is used by Stern's algorithm. We will refer to this altered weight as *block-weight.* Taking into account the special form of P also has other beneficial effects for the attacker. In particular, Algorithm 2 has a higher probability of success when the rank effects of the inclusion of blocks of ℓ columns (instead of individual columns) are considered, since it is much less likely for these blocks to be totally linearly dependent on each other, for reasons other than the overall block structure of the matrix.

The modified version of Stern's algorithm proceeds as shown in Algorithm 3. Note the Stern's algorithm window size will be denoted L, instead of the standard l, to avoid confusion with the granularity.

Algorithm 3: Modified Stern's Algorithm

Input: a matrix G_{pub}, parameters p, t, L, ℓ

Output: a vector in the row space of G_{pub} which has block-weight t

1. Permute the columns of G_{pub} :
$$G'_{pub} = G_{pub}P',$$
where P' is a permutation matrix consisting of $\ell \times \ell$ blocks which are either zero or the identity, but otherwise chosen randomly.
2. Check that the first k columns of the new matrix G'_{pub} form an invertible matrix A. If A is not invertible, go back to step 1.
3. Left-multiply by A^{-1}, resulting in a matrix of the form
$$M = A^{-1}G'_{pub} = \left[I_k \mid Q\right].$$
4. Search for low-weight row-vectors among linear combinations involving small subsets of the rows of M:
   (a) Divide the rows of M into two equal length lists, i.e.,
   for $0 < i \leq \frac{k}{2\ell}$, and for $B = (b_1, .., b_\ell) \in \mathbb{F}_2^\ell$
   $$x_{i,B} = \sum_{r=1}^{\ell} b_r \text{row}_{i\ell+r}(M).$$
   Similarly, for $\frac{k}{2\ell} < j \leq \frac{k}{\ell}$
   $$y_{j,B} = \sum_{r=1}^{\ell} b_r \text{row}_{j\ell+r}(M).$$
   (b) Compute each possible sum of all subsets of size p of the $x_{i,B}$, as well as for all possible sums of p of the $y_{j,B}$. Check for collisions on bits $(k+1), \ldots, (k+L)$:
   $$\text{bits}_{k+1,\ldots,k+L\ell}(x_{i_1,B_1} + \ldots + x_{i_p,B_p}) = \text{bits}_{k+1,\ldots,k+L\ell}(y_{j_1,B_1} + \ldots + y_{j_p,B_p}).$$
   (c) When such a collision is found, compute the sum s of the $2p$ colliding row vectors
   $$s = x_{i_1} + \ldots + x_{i_p} + y_{j_1} + \ldots + y_{j_p}.$$
   If the block-weight of any such s is equal to t return sP'. Otherwise, go back to step 1.

We now give an analysis of the complexity of obtaining the full list of target columns using this modified Stern's algorithm. Note that this analysis is only approximate, a tighter analysis may be possible using techniques similar to those outlined in section 5 of [16]. For each block-weight t target vector g, the search will succeed if and only if gP' has block-weight p on its first $\frac{k}{2}$ bits, block-weight p on the next $\frac{k}{2}$ bits, and block-weight 0 on the next L bits. For a randomly chosen P' this probability is

$$\mathrm{Prob}(n,k,p,\ell,L,t) = \binom{n/\ell}{t}^{-1}\binom{k/(2\ell)}{p}^{2}\binom{(n-k-L)/\ell}{t-2p},$$

and the equivalent probability for an attack on H_{pub} is

$$\mathrm{Prob}(n,n-k,p,\ell,L,t) = \binom{n/\ell}{t}^{-1}\binom{(n-k)/(2\ell)}{p}^{2}\binom{(k-L)/\ell}{t-2p}.$$

The approximate number $\mathcal{D}$ of distinct target vectors of a given weight t is

$$\mathcal{D}_{sig} \approx \binom{(k_w+n_w)/\ell}{t}\left(2^{\ell}-1\right)^{t}\cdot 2^{-n_w},$$

for signature, and for encryption

$$\mathcal{D}_{enc} \approx \binom{(n_1+k_1)/\ell}{t}\left(2^{\ell}-1\right)^{t}\cdot 2^{-k_1}.$$

The expected number $\mathcal{E}$ of target vectors required for a successful attack is

$$\mathcal{E}_{sig} \approx \left\lceil \frac{\log\left(\frac{k_w}{k_w+n_w}\right)}{\log\left(\frac{k_w+n_w-t\ell}{k_w+n_w}\right)} \right\rceil,$$

for signature, and for encryption

$$\mathcal{E}_{enc} \approx \left\lceil \frac{\log\left(\frac{n_1}{n_1+k_1}\right)}{\log\left(\frac{n_1+k_1-t\ell}{n_1+k_1}\right)} \right\rceil.$$

The total number of iterations of the modified Stern's algorithm is therefore

$$i_{sig} \approx \left\lceil \frac{\log(\frac{k_w}{k_w+n_w})}{\log(\frac{k_w+n_w-t\ell}{k_w+n_w})} \right\rceil \cdot \binom{(k_w+n_w)/\ell}{t}^{-1}\left(2^{\ell}-1\right)^{-t} 2^{n_w} \cdot \binom{n/\ell}{t}\binom{k/(2\ell)}{p}^{-2}\binom{(n-k-L)/\ell}{t-2p}^{-1},$$

and

$$i_{enc} \approx \left\lceil \frac{\log(\frac{n_1}{n_1+k_1})}{\log(\frac{n_1+k_1-t\ell}{n_1+k_1})} \right\rceil \cdot \binom{(n_1+k_1)/\ell}{t}^{-1}\left(2^{\ell}-1\right)^{-t} 2^{k_1} \cdot \binom{n/\ell}{t}\binom{(n-k)/(2\ell)}{p}^{-2}\binom{(k-L)/\ell}{t-2p}^{-1}.$$

5 Experimental Results

We implemented the attacks described in the previous section on a standard laptop with a 2.2 GHZ Intel core i7 processor. We used the parameters suggested by Gligoroski et al. for 80 bits of security. Concretely, for encryption $n = 1160, k = 160, \ell = 2, w = 17$, with $K = (32, 8, 8, ..., 8)$ and $N = (32, 32, ..., 32, 488)$. We used parameters $(t, p, L) = (11, 1, 9)$ for the modified Stern's algorithm, which needed approximately 1000 iterations in our trials. The predicted value from the analysis in the previous section was 2500. The total wall time for the computation to recover a private key was on average less than 2 hours.

For signatures, we have $n = 650, k = 306, \ell = 2, w = 6$, with $K = (84, 48, 48, 48, 48, 30)$ and $N = (48, 48, 48, 48, 48, 104)$. The modified Stern parameters we used were $(t, p, L) = (40, 1, 7)$. With such a high value for t, a higher number of iterations were needed, usually less than 10000 (the predicted value was around 4900). The total wall time was again less than 2 hours on average.

6 Countermeasures

Attempts to increase the security of McEliece Escher by altering the parameters are severely constrained by the requirement that ρ^{k_1} be small for encryption and that $(2/\rho)^{n_w}$ be small for signatures.

One possiblility would be to try to decrease ρ (or $2/\rho$), as appropriate, to allow k_1 or n_w to increase. This, however, turns out to be counterproductive. Due to the attack in Section 4.1, we see what really matters for security is that k_1/ℓ be large for encryption, or n_w/ℓ be large for signatures. Asymptotically, there will be 2^ℓ vectors in the row space of H_{pub} of block-weight no more than $k_1/\ell + 1$ and 2^ℓ vectors in the row space of G_{pub} of block-weight no more than $n_w/\ell + 1$. The factor of 2^ℓ will make up for the increased cost per iteration of the modified Stern's algorithm with $p = 1$, but the probability of success per iteration will remain at approximately $(\frac{k}{n})^{k_1/\ell}$ for encryption and $(\frac{n-k}{n})^{n_w/\ell}$ for signatures. Encryption requires $(\rho^\ell)^{k_1/\ell}$ to be small for efficiency and k_1/ℓ to be large for security. Thus the ideal value for ρ and ℓ would minimize ρ^ℓ. Likewise, the signature scheme requires $((\frac{2}{\rho})^\ell)^{n_w/\ell}$ to be small for efficiency and n_w/ℓ to be large for security. Hence, the ideal value for ρ and ℓ would minimize $(\frac{2}{\rho})^\ell$.

While it is possible to decrease ρ (or $\frac{2}{\rho}$) by increasing ℓ, the consequence is that ρ^ℓ and $(\frac{2}{\rho})^\ell$ both increase at least linearly in ℓ for error sets of the proper form (for security, the generalized error set cannot impose linear constraints on the error vector, e.g. by forcing a bit of the error vector to always be 0). Thus, fixing $\frac{n}{k}$ and the security level, we find that the cost of decryption increases when we increase ℓ.

A better idea is to greatly increase n_w for encryption and k_w for signatures. This works by making $\frac{k}{n}$ very small for encryption and $\frac{n-k}{n}$ very small for signatures. In the context of an information set decoding attack, this has the effect of decreasing the probability that a given nonzero bit (or ℓ-bit block) of a target vector will be placed outside the information set by a randomly chosen (block) permutation. This is a much better solution for signatures than for encryption. For typical parameters, the modified Stern's algorithm requires ~ 30 nonzero blocks to fall outside the information set when attacking a signature. Thus, bringing the cost of the attack from $\sim 2^{30}$ to $\sim 2^{80}$ should only require $\frac{n-k}{n}$ to fall from about 0.5 to about 0.15. That is, the size of the 80-bit-secure code increases from a 650×304 bit generator matrix to a 2000×1654 bit generator matrix. For attacking typical encryption parameters, the modified Stern's algorithm only requires ~ 6 nonzero blocks to fall outside the information set. This means $\frac{k}{n}$ needs to fall from about 0.15 to 0.0005. The result is that for an 80-bit-secure code, the size would increase from 1160×160 to $300,000 \times 160$.

There is however an additional complication created by the above countermeasure for signatures. A code with error set $E = \{00, 01, 10\}$ can be trivially broken whenever $\frac{n-k}{n} < 0.5$ due to the attack described at the end of Section 3. This attack may be generalized to apply to other error sets, whenever there is a linear projection from $\mathbb{F}_2^{\ell} \to \mathbb{F}_2^{\ell'}$ with $\ell' \leq \frac{k}{n}\ell$ such that an element of $\mathbb{F}_2^{\ell}$ with a certain fixed projection onto $\mathbb{F}_2^{\ell'}$ is a member of the error set with very high probability. Thus in order to avoid attack, the error set must be chosen so that there is no such projection. We have not found any way to do this that makes the honest party's signing operation (list decoding for signatures) asymptotically more efficient than both attacks (ISD for the error vector and ISD for the private key.)

7 Conclusion

We demonstrate practical attacks on the proposed parameters of McEliece Escher. The poor choice of parameters is a demonstration of the general principle that code-based schemes should be designed in such a way as to avoid all practical distinguishers on the public key, since distinguishers can often be modified, at little cost, to create private-key recovery attacks. Additionally, our cryptanalysis demonstrates that information set decoding techniques can be modified to take advantage of code-based schemes whose private keys are disguised by a structured, rather than a completely random, permutation matrix. The recent cryptanalysis of cyclosymmetric-MDPC McEliece by Perlner [17] is another example of this general principle. This technique is especially effective in creating signature forgeries.

For encryption, it appears the above pitfalls can be compensated for, by simply making the parameters of McEliece Escher larger. However, this requires making the keys at least two orders of magnitude larger. This is a major burden on an already inefficient scheme. Asymptotically, these modifications can only make the complexity of a key-recovery attack quasi-polynomially worse than the complexity of decryption by the honest party.

References

1. McEliece, R.J.: A Public-Key Cryptosystem Based On Algebraic Coding Theory. Deep Space Network Progress Report **44** (1978) 114–116
2. Misoczki, R., Tillich, J.P., Sendrier, N., Barreto, P.S.L.M.: MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes. Cryptology ePrint Archive, Report 2012/409 (2012) http://eprint.iacr.org/.
3. Gaborit, P., Murat, G., Ruatta, O., Zemor, G.: Low Rank Parity Check codes and their application to cryptography. In Lilya Budaghyan, Tor Helleseth, M.G.P., ed.: The International Workshop on Coding and Cryptography (WCC 13), Bergen, Norway (2013) 13 p. ISBN 978-82-308-2269-2.
4. Gaborit, P., Ruatta, O., Schrek, J., Zmor, G.: RankSign: An Efficient Signature Algorithm Based on the Rank Metric. In Mosca, M., ed.: Post-Quantum Cryptography. Volume 8772 of Lecture Notes in Computer Science. Springer International Publishing (2014) 88–107
5. Gligoroski, D., Samardjiska, S., Jacobsen, H., Bezzateev, S.: McEliece in the World of Escher. Cryptology ePrint Archive, Report 2014/360 (2014) http://eprint.iacr.org/.
6. Gligoroski, D.: A New Code Based Public Key Encryption and Signature Scheme Based on List Decoding. (Presented at "Workshop on Cybersecurity in a Post-Quantum World," NIST, Gaithersburg MD, USA)
7. Prange, E.: The Use of Information Sets in Decoding Cyclic Codes. Information Theory, IRE Transactions on **8** (1962) 5–9
8. Lee, P., Brickell, E.: An Observation on the Security of McEliece's Public-Key Cryptosystem. In Barstow, D., Brauer, W., Brinch Hansen, P., Gries, D., Luckham, D., Moler, C., Pnueli, A., Seegmller, G., Stoer, J., Wirth, N., Gnther, C., eds.: Advances in Cryptology EUROCRYPT 88. Volume 330 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (1988) 275–280
9. Leon, J.: A Probabilistic Algorithm for Computing Minimum Weights of Large Error-correcting Codes. Information Theory, IEEE Transactions on **34** (1988) 1354–1359
10. Stern, J.: A Method for Finding Codewords of Small Weight. In Cohen, G., Wolfmann, J., eds.: Coding Theory and Applications. Volume 388 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (1989) 106–113
11. Finiasz, M., Sendrier, N.: Security Bounds for the Design of Code-Based Cryptosystems. In Matsui, M., ed.: Advances in Cryptology ASIACRYPT 2009. Volume 5912 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2009) 88–105
12. Bernstein, D., Lange, T., Peters, C.: Smaller Decoding Exponents: Ball-Collision Decoding. In Rogaway, P., ed.: Advances in Cryptology CRYPTO 2011. Volume 6841 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2011) 743–760
13. May, A., Meurer, A., Thomae, E.: Decoding Random Linear Codes in $\tilde{O}(2^{0.054n})$. In Lee, D., Wang, X., eds.: Advances in Cryptology ASIACRYPT 2011. Volume 7073 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2011) 107–124
14. Becker, A., Joux, A., May, A., Meurer, A.: Decoding Random Binary Linear Codes in $2^{n/20}$: How $1 + 1 = 0$ Improves Information Set Decoding. In Pointcheval, D., Johansson, T., eds.: Advances in Cryptology EUROCRYPT 2012. Volume 7237 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2012) 520–536
15. Landais, G., Tillich, J.P.: An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional Codes. In: Post-Quantum Cryptography. Springer (2013) 102–117
16. Otmani, A., Tillich, J.P.: An efficient attack on all concrete kks proposals. In Yang, B.Y., ed.: Post-Quantum Cryptography. Volume 7071 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2011) 98–116
17. Perlner, R.: Optimizing Information Set Decoding Algorithms to Attack Cyclosymmetric MDPC Codes. In Mosca, M., ed.: Post-Quantum Cryptography. Volume 8772 of Lecture Notes in Computer Science. Springer International Publishing (2014) 220–228

Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 43 (2016) 13 – 16

www.elsevier.com/locate/procedia

14th CIRP Conference on Computer Aided Tolerancing (CAT)

Interoperability: linking design and tolerancing with metrology

Edward Morse* [a], Saeed Heysiattalab [a], Allison Barnard-Feeney [b], Thomas Hedberg, Jr. [b]

[a] Center for Precision Metrology, UNC Charlotte, Charlotte, NC 28223 USA
[b] National Institute for Standards and Technology, Gaithersburg, MD 20899 USA

* Corresponding author. Tel.: +1-704-687-8342; fax: +1-704-687-8255. *E-mail address:* emorse@uncc.edu

Abstract

On October 30, 2014 the American National Standards Institute (ANSI) approved QIF v 2.0 (Quality Information Framework, version 2.0) as an American National Standard. Subsequently in early 2016 QIF version 2.1 was approved. This paper describes how the QIF standard models the information necessary for quality workflow across the full metrology enterprise. After a brief description of the XML 'language' used in the standard, the paper reports on how the standard enables information exchange among four major activities in the metrology enterprise (product definition; measurement planning; measurement execution; and the analysis and reporting of the quality data).

© 2016 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the organizing committee of the 14th CIRP Conference on Computer Aided Tolerancing

Keywords: Standards; Metrology Data; Interoperability

1. Introduction

Metrology has – at times – been placed in the role of quality checking, the final step of conformance testing before a product is deemed acceptable. The more advanced manufacturer of components realizes that there is more value in metrology than a simple final-acceptance check. Using metrology information to improve the manufacturing process by controlling and reducing product variability has become an integral part of modern, high-quality manufacturing. The management of variability is more easily performed in organizations that are integrated vertically because different parts of the process 'belong' to the same company. In a flatter, more distributed, manufacturing environment this task is much harder, as each participant (company, division, etc.) may optimize their part of the process to the detriment of the complete process's quality. Standardization is recognized as a means to allow interoperability across a variety of platforms in almost countless contexts, from standardized reporting of gasoline octane content based on underlying test methods to the height of work surfaces, including office desks and commercial kitchen counters. The specific focus of this paper is Product and Manufacturing Information (PMI) for discrete products.

The goal of the Quality Information Framework (QIF) [1,2] is to support the transfer of information and data related to metrology through the entire product process, from design to manufacture to the archival and analysis of data related to the products. This paper will provide a high-level overview of the current QIF structure and the various components of this structure. We will then focus on one particular area (i.e., metrology resources) in more detail, both to examine the thinking behind the development of this area and to reveal how we envision end users realizing the benefits of the QIF. We will conclude with some specific attributes of the metrology resources structure that relate to large scale and portable metrology systems.

Acronyms

QIF	Quality Information Framework
XML	Extensible Markup Language
PMI	Product and Manufacturing Information

2212-8271 © 2016 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the organizing committee of the 14th CIRP Conference on Computer Aided Tolerancing
doi:10.1016/j.procir.2016.04.106

2. The Quality Information Framework (QIF)

The QIF captures the natural structure of information flow related to part geometry: from the initial description of the geometry and the supplemental information that is provided by the designer all the way to the statistical analysis of inspection results for multiple workpieces. At each step along the way, the necessary information is captured in a standard format, allowing greater flexibility in choosing the tools used in the next process step. The standard format is defined using Extensible Markup Language (XML) and demonstrated using a variety of tools that support the QIF standard [3].

2.1. XML schemas and files

XML is readable by both humans and computers. The same file that is used for modeling a particular situation can also be examined by a person looking for particular information. This is similar to the use of HTML for web pages. The two main types of files that we will consider are XML Schema Definitions, herein schemas, and XML files. The QIF consists of schemas, which define templates for the type of information needed in each step. When QIF is used, an XML file is generated, which could be evaluated to see if the file conforms to the schema. The file fragments below show a simple example of the relationship between the schema definition and an instance of a particular use of the schema.

Table 1. XML schema and XML file example.

```
<xs: element name="Contact">
  <xs: ComplexType>
     <xs: sequence>
       <xs: element name="name" type="xs:string"/>
       <xs: element name="FamilyName" type="xs:string"/>
       <xs: element name="Address" type="xs:string"/>
     </xs: sequence>
  </xs: ComplexType>
</xs: element>
```

Fragment of an XML schema definition

```
<Contact>
    <name>Ed</name>
    <FamilyName>Morse</FamilyName>
    <Address>UNC Charlotte</Address>
</Contact>
```

Resulting XML file instance

In Table 1, the schema defines what information is needed (i.e., it's a template), and the user puts the appropriate information in an instance XML file. Many XML files could be created that conform to the schema template.

2.2. The QIF schemas

The QIF schemas are used at the conclusion of each step in the product-quality process so that the data passed to the next step has a standard format. For example, when the design of the part geometry and tolerances is concluded, it may be transferred to metrology in a native format, or in another standard format such as ISO 10303-202 Managed Model-based 3D Design, known as STEP AP242 [4]. It may also be exported according to the QIF MBD (model-based definition) schema. This ensures automated processes that determine measurement requirements, based on the part geometry and tolerances, have access to the information needed to complete this task. Note that as in the above example, the schema doesn't describe the geometry – simply how the geometry is captured in the file. The other QIF application schemas used are QIF Resources, QIF Rules, QIF Plans, QIF Results, and QIF Statistics. The execution of measurement programs within the QIF uses DMIS version 5.2 [5]. These application schemas rely on common elements that are captured in the QIF libraries, as shown in Fig. 1.

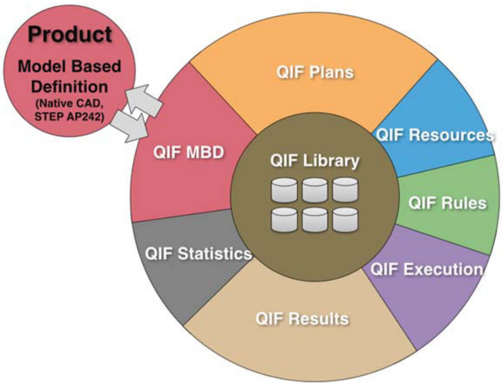


Fig. 1. A representation of the QIF schemas and the supporting libraries

The role of these data models is apparent when we think about the quality process: given the part geometry and tolerances, what is needed to develop a measurement plan? The identification of the part attributes that must be measured is determined by the quality requirements and by the manufacturing processes used. This information is captured in the "whats" portion of the QIF Plans schema. Once it is known what must be inspected, the information about available metrology resources (QIF Resources) and rules for applying these resources (QIF Rules) must be applied to complete the "hows" portion of the QIF Plans. Now the measurement plan is complete, this is implemented using DMIS and the results are captured in accordance with the QIF Results schema. Finally, post processing can be accomplished according to the QIF Statistics schema. As a reminder to the reader, each of these schemas simply provides a template for moving information. Fig. 2 shows the alignment of the various schema definitions to the different tasks in the metrology lifecycle.

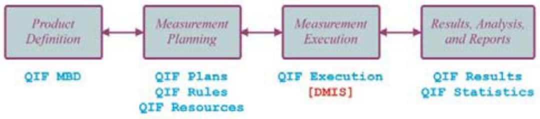


Fig. 2. The parts of QIF related to the overall metrology workflow

3. Metrology Resources

In this section, recent work in the area of QIF Resources is described. Constructing a template that will have a logical space for the important attributes of common metrology instruments is desired in developing a schema for metrology resources. One long-term objective in the development of a comprehensive QIF Resources schema is the ability to capture a metrology company's entire instrument catalog within the template. Similarly, a manufacturing organization could have information about all of their instruments stored in this same format. This would enable different software to browse through the inventory to determine what instruments are most appropriate for various measuring tasks, which instruments will soon be in need of calibration, and other automated tasks.

3.1. Structure

The structure of the metrology resources schema is a hierarchy of instruments and sensors, each containing descriptive attributes of these resources.

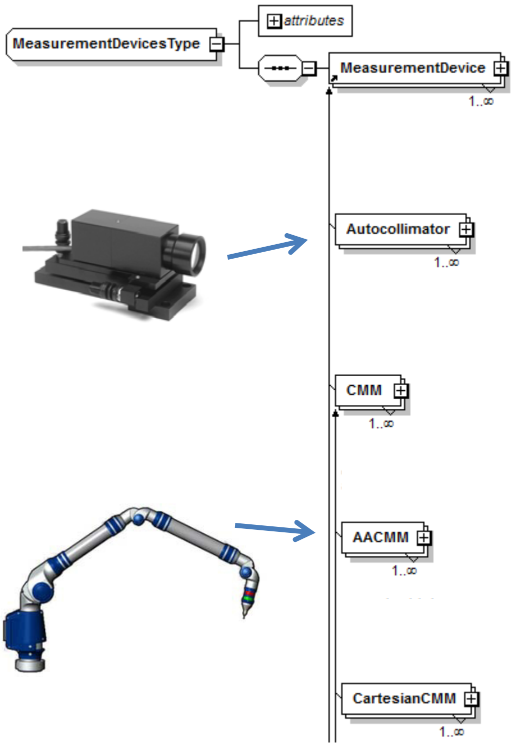


Fig. 3. Part of the Measurement Resources hierarchy

The highest level of this hierarchy is Measurement Resources, followed by the next level containing the subtypes of Version information, Fixtures, Tools, Detachable Sensors, and Measurement Devices. Part of the measurement devices hierarchy from QIF version 2.1 is shown in Fig. 3. This figure shows how both an Autocollimator and CMM are modeled as resources, and the CMM has multiple subtypes below the main CMM type.

3.2. CMM-specific attributes

The CartesianCMM type shown in Fig. 3 contains attribute information that is relevant to these instruments. Specific examples of these attributes include: the home location of the CMM, the maximum permitted workpiece mass, the motion speeds (both DCC and joystick), machine accuracy, and others. A data model that supports this level of detail is useful when selecting a piece of measuring equipment and developing the measuring plan for the equipment.

The CMM type is an extension of the base type of `UniversalDeviceType`, which in turn is an extension of the `MeasurementDeviceType`. This is important because common attributes to all non-manual measuring devices that have a measuring volume can be captured in the Universal device type. This prevents these attributes from being repeated at many places through out the schema definition. For example, different types of measuring volumes are described for "universal devices," including a Cartesian (box shaped) volume, a spherical volume, and a cylindrical volume. An explicit geometric model of the measuring volume can be defined if the volume does not have one of these shapes, such as when the usable measuring volume is reduced by a tool-changing rack.

4. Building Trust and Traceability

Now that the structure of QIF and some details of the data model have been explained, the method of determining the validity of data shared using this model is described. Ensuring complete data integration of both data trust and traceability is important to manufacturing industries. Those organizations must be able to determine data declarations, who did what to the data, when they did it, and potentially why it was done. Both regulated and non-regulated industries need effective and efficient processes for data trust and traceability. Regulated industries (e.g., aerospace, automotive, medical) focus significant resources on data trust and traceability to ensure they comply with the appropriate public-safety oversight. Manufacturers in both regulated and non-regulated industries care about data trust and traceability to reduce product-liability exposure in their supply chains and the public.

Ouertani *et al* [6] suggest the following questions must be answered to support data trust and traceability:

- What product knowledge is created or represented?
- Who are the actors playing different roles in creating, using, or modifying product knowledge?
- Where is the product knowledge created and located?
- How is the product knowledge being created or modified?
- Why was certain product knowledge created or modified?
- When was the product knowledge created or modified?

QIF version 2.1 supports the ability to embed digital signatures using Private Key Infrastructure methodology from the X.509 standard [7]. QIF version 2.1 introduces two elements to the schema – (1) a `signature` block and (2) a set of elements for traceability. The `signature` block allows the user to add the *who* and *when* to the QIF document. The traceability elements allow the user to add the *what* to the QIF document. Using the `signature` block and traceability elements together enables full traceability of who did what to the QIF data and when it was done. This traceability supports the end-user's ability to determine if the data in the QIF document may be trusted.

5. QIF Benefits to the Product Lifecycle

Standardized metrology data across the product lifecycle, and tasks, such as measurement planning, can be automated is the benefit of QIF. Any software that can read part files in the QIF MBD format, as well as the QIF Resources and QIF Rules files for the organization, could generate measurement plans and send them to measuring equipment using the QIF Plans schema.

As described in Section 2.2, QIF's concept of identifying a metrology "catalog" both of resources and rules combined in a plan brings a significant benefit to the product lifecycle. Knowing what resources are available to an organization and knowing the metrology rules that constrain the inspection capabilities for a given part enables the organization to determine if upstream (e.g., design, manufacturing) decisions comply with metrology's needs. QIF's inherent structure supports efficient and effective knowledge capture of metrology capabilities. This knowledge could be leveraged to determine if a design or manufacturing decision being made will detrimentally affect the inspection process. This would reduce waste and cost significantly.

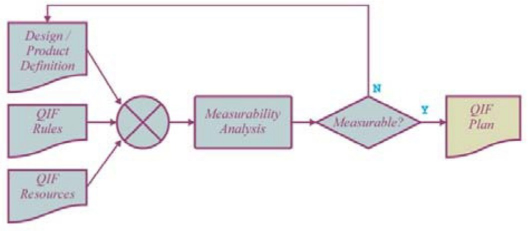


Fig. 4. Process flow for analyzing measurability using QIF

For example, a design engineer could follow the example process flow shown in Fig. 4 to determine if the product definition is complete and measureable. The engineer would collectively examine the product definition, pre-defined QIF rules, and the catalog of metrology resources represented in QIF resources. The engineer would then complete an analysis prior to releasing the design to fabrication to ensure the product could be inspected using the pre-defined metrology rules and available resources. If the product is measureable, a QIF plan would be the output. If the product is not measureable, the engineer would make changes to the product definition until the product becomes measureable. The result is a design that complies with metrology's needs such that the information and production definition is in a state that metrology can effectively and efficiently use for completing the inspection process. Using a "Design for Inspection" approach built around QIF ensures that the product definition is correct at release and eliminates the need to iterate the handoff of the product definition between design and supply chain. This reduces the time wasted by rework, while also reducing production costs due to missing information not being discovered until after the product has been fabricated.

6. Conclusion

This paper presented an overview of the QIF standard, a more in-depth discussion of the QIF Resources schema definition, a discussion of trust and traceability issues and their support in QIF documents, and an example of the type of application development that can be enabled when QIF is used to capture the metrology information throughout the product-design workflow. As the standard matures, and more commercial software support the reading and writing of QIF-compliant files, the goal of a *digital thread* [8] linking all aspects of the product lifecycle will come closer to reality. This powerful set of standards, describing data models for all of the metrology-related aspects of the product process flow, is already instrumental in providing new opportunities for the management of metrology across a variety of platforms.

Acknowledgements

The authors wish to acknowledge the DMSC and the QIF working groups for their continued effort in the development of QIF standards. This work has been supported in part by a cooperative research agreement (NIST grant number 70NANB14H254) between UNC Charlotte and NIST.

References

[1] ANSI/QIF version 2.0 – 2014
[2] ANSI/QIF version 2.1 – 2016
[3] HM Huang, J Michaloski, D Campbell, R Stone, T Kramer, C Brown, R Brown, G Tatarliev. NISTIR 8102, End-to-end Demonstration of the Quality Information Framework (QIF) Standard at the International Manufacturing Technology Show (IMTS) 2014
[4] ISO 10303-242, 2014. Industrial automation systems and integration – Product data representation and exchange – Part 242: Application protocol: Managed model-based 3D design. International Organization for Standardization, Geneva, Switzerland.
[5] ANSI/DMIS 105.2, Part 1 – 2009
[6] Ouertani, M. Z., Baïna, S., Gzara, L., & Morel, G. (2011). Traceability and management of dispersed product knowledge during design and manufacturing. Computer-Aided Design, 43(5), 546-562. doi:http://dx.doi.org/10.1016/j.cad.2010.03.006
[7] ISO/IEC 9594-8:2014 Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks. International Standards Organization, Geneva.
[8] Hedberg Jr, T.D., Lubell, J., Fischer, L., Maggiano, L., Barnard-Feeney, A. (2016). Testing the Digital Thread in Support of Model-Based Manufacturing and Inspection. *Journal of Computing and Information Science in Engineering*, 16(2), 1-10. doi:10.1115/1.4032697

PERFORMANCE EVALUATION OF A LASER TRACKER HAND HELD TOUCH PROBE

B. Muralikrishnan, C. Blackburn, P. Rachakonda, and D. Sawyer
Semiconductor and Dimensional Metrology Division
National Institute of Standards and Technology
Gaithersburg, MD 20899

INTRODUCTION

Hand held touch probes and laser scanners are increasing the scope and applicability of laser trackers. While methods to evaluate the performance of laser trackers in conjunction with spherically mounted retroreflectors (SMRs) are well established, methods for evaluating the performance of hand held probes [1-2] are still under discussion within ISO 10360-10. We discuss the performance of a hand held touch probe in this paper. Single point articulation tests (SPATs) are commonly employed both to calibrate and to test these devices. We have modeled a hand held touch probe and subsequently performed simulations to understand the influence of different error parameters on measured coordinates in two different configurations of SPATs. The overall objective is to develop detailed uncertainty budgets for measurements made using the hand held touch probe. We present preliminary simulation and experimental results here as a first step towards realizing that objective.

THE HAND HELD TOUCH PROBE

There are several designs of hand held touch probes in the market. A schematic of the hand held touch probe under evaluation is shown in Fig. 1. The laser tracker measures the position of the retroreflector located in the hand held touch probe. An orifice at the apex *o* of the retroreflector allows a portion of the laser beam to travel further onto a charge-coupled device (CCD). The position of the laser spot on the CCD determines the pitch angle β (rotation about the y axis of the hand held touch probe) and yaw angle γ (rotation about the z axis). Roll angle α (rotation about the *x* axis) is determined by a gravity sensor. The link lengths *a* (along the *x* axis), *b* (along the *y* axis, not shown in the figure because it is nominally zero in this configuration), and *c* (along the *z* axis) are determined through a calibration procedure performed prior to measurement. Using the three measured angles and three link lengths, the coordinates of the stylus tip *P* can be determined through a geometric transformation. The hand held touch probe also has a separate yaw joint. While we use this yaw joint to orient the retroreflector towards the tracker between the different SPATs, we have not exercised the yaw joint during a SPAT; we therefore do not consider this in our model. Simulations and experiments were performed using the horizontal stylus only.

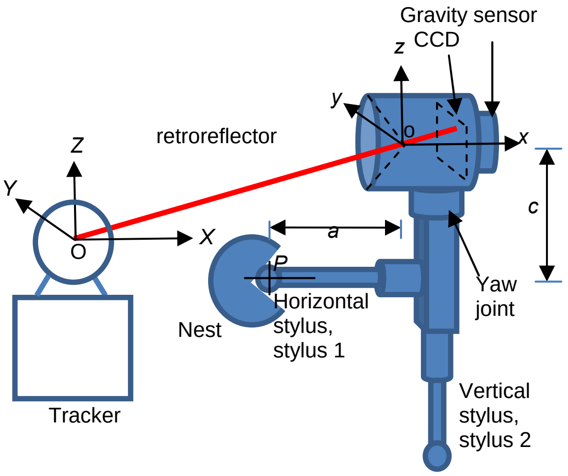


FIGURE 1. Schematic of the hand held touch probe

COORDINATE SYSTEMS

We define two coordinate systems, one on the tracker (*XYZ*) and another on the hand held touch probe (*xyz*). The origin of the coordinate system on the hand held touch probe is located at the apex of the retroreflector. The *x* axis is normal to the plane of the CCD while the *z* axis is parallel to the long handle of the hand held touch probe as shown in Fig. 1. Let the position of the retroreflector as recorded by the tracker in spherical coordinates be (*R*, *H*, *V*). In order to determine the coordinates of the stylus tip *P* in the laser tracker coordinate system, we employ the following sequence of translations and rotations.

Muralikrishnan, Balasubramanian; Blackburn, Christopher; Rachakonda, Prem; Sawyer, Daniel.
"Performance evaluation of a laser tracker hand held touch probe."
Paper presented at the Annual Meeting of the ASPE 2015, Austin, TX, Nov 2-Nov 5, 2015.

Let the retroreflector of the hand held touch probe first be located at (*R*, 0, 0) as shown in Fig. 2(a). Let the orientation of the hand held touch probe be such that roll, pitch, and yaw angles are zero at this position. The stylus tip coordinate is known in the tracker frame at this position and is given by (*R*-*a*, -*b*, -*c*). The hand held touch probe is then rotated by an angle *V* about the *Y* axis and then by an angle *H* about the *Z* axis to the position shown in Fig. 2(b). The hand held touch probe is then rotated about *its x* axis by the roll angle (Fig. 2(c)) and subsequently about *its y* axis by the pitch angle (Fig. 2(d)) and then about *its z* axis by the yaw angle (not shown in Fig. 2). The resulting coordinate for the stylus tip is the desired coordinate in the laser tracker coordinate system.

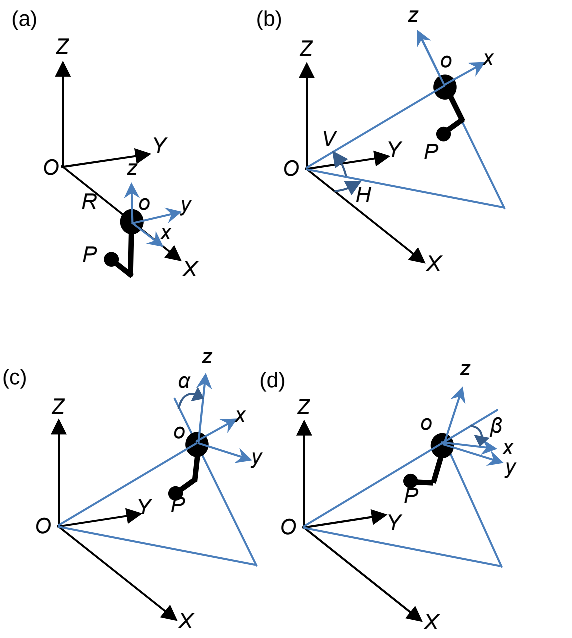


FIGURE 2. Transformations to calculate stylus tip coordinate in laser tracker frame (a) retroreflector located at (R, 0, 0) with hand held touch probe oriented such that there is no roll, pitch, or yaw, (b) hand held touch probe rotated about Y axis by angle V and then about the Z axis by angle H, (c) hand held touch probe rotated about its x axis by the roll angle, (d) hand held touch probe rotated about its y axis by the pitch angle

Single point articulation tests

Two configurations of SPATs are considered in this study; they are shown in Fig. 3. In each case, with the stylus tip located in the nest so that the center of the stylus tip remains in the same position during articulation, the hand held touch probe is rotated about each of the three axes to the extent possible, which is ±30° for the pitch and yaw axes and ±60° for the roll axis. While the hand held touch probe itself is capable of 360° along the roll axis, physical limitations in the test setup only allowed for ±60° in that axis. The nominal values for link lengths *a*, *b*, and *c* are 85 mm, 0, and 85 mm respectively for SPAT #1, similar to the horizontal configuration shown in Fig. 1 and in Fig. 3(a), and 85 mm, 40 mm, and 85 mm respectively for SPAT #2 as shown in Fig. 3(b). The nest was located about 2 m from the laser tracker.

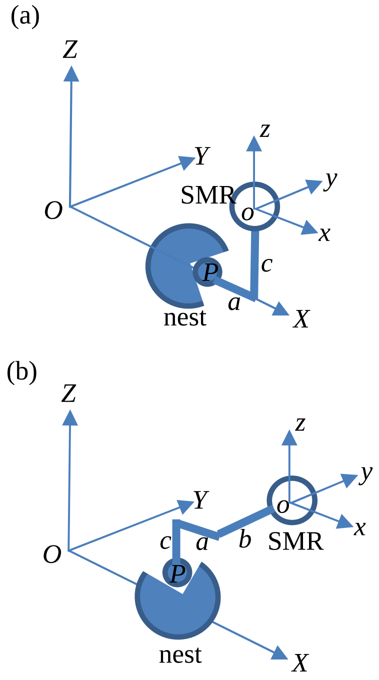


FIGURE 3. Two configurations of SPATs shown (a) SPAT #1 (a = 85 mm, b = 0, c = 85 mm) and (b) SPAT #2 (a = 85 mm, b = 40 mm, c = 85 mm)

Errors in the link lengths and in the measured angles produce errors in the measured coordinates. In order to determine reasonable values for the parameters to be used as input to the simulations, two different experiments were performed. First, the manufacturer suggested calibration procedure was performed several times to determine the one standard deviation repeatability in the link lengths. This procedure involves performing a SPAT while exercising the yaw joint between the different orientations of the hand held touch probe. The manufacturer's software considers the different stylus tip coordinates obtained during the SPAT and the laser tracker's determination of the nest coordinate obtained using an SMR to evaluate the link lengths. Multiple such calibrations resulted in link length repeatability on the order of 10 µm. Although it is possible there are other sources of systematic error that will result in a larger uncertainty in the link lengths, the one standard deviation repeatability of 10 µm is considered as the standard uncertainty in each of the three link lengths *a*, *b*, and *c*, and propagated to the stylus tip in the simulations.

In order to estimate the uncertainty in the roll, pitch, and yaw angles, the hand held touch probe was mounted on a precision air bearing rotary table and the yaw angle of the hand held touch probe was compared against the encoder readings of the rotary table. That experiment indicated a yaw angle error on the order of 1 mrad, which is considered as the uncertainty in each of the three angles, and propagated to the stylus tip in the simulations. It should be noted that the roll angle is a coarser measurement in comparison to pitch and yaw; at this time, we have not quantified the errors associated with the roll angle and therefore simply use the same value as obtained for yaw.

Results and discussion

As mentioned in the previous section, the purpose of the simulations is to understand the influence of errors in each of the six input parameters on the stylus tip coordinate for the two different SPATs. A SPAT can be performed in either the absolute mode or in the relative mode. In the absolute mode, the coordinates of the stylus tip for the various orientations in a SPAT are compared to the coordinate as measured using an SMR mounted on the nest. In the relative mode, the coordinates of the stylus tip for the various orientations in a SPAT are compared against each other.

The stylus tip size in our hand held touch probe was 6 mm in diameter. The SPAT is typically performed using a manufacturer provided nest that has a conical seat in a 1.5 in spherical shell. When the stylus tip is located in the conical seat, the center of the tip is ideally also the center of the spherical shell, and the coordinate of that point can be determined using a 1.5 in SMR. In some situations, it may not be physically possible to measure the coordinate of the nest using an SMR and therefore relative SPATs are sometimes performed.

TABLE 1. Simulation results for SPAT #1 analyzed in absolute mode and in relative mode. All units in millimeters.

	SPAT #1 in absolute mode									SPAT #1 in relative mode								
	Roll test			Pitch test			Yaw test			Roll test			Pitch test			Yaw test		
	X	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*
a	0.01	0.00	0.00	0.01	0.00	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.01	0.00
b	0.00	0.01	0.01	0.00	0.01	0.00	0.01	0.01	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.01	0.00	0.00
c	0.00	0.01	0.01	0.01	0.00	0.01	0.00	0.00	0.01	0.00	0.01	0.00	0.01	0.00	0.00	0.00	0.00	0.00
α	0.00	0.08	0.07	0.00	0.11	0.00	0.00	0.08	0.04	0.00	0.02	0.07	0.00	0.05	0.00	0.00	0.00	0.04
β	0.08	0.07	0.09	0.12	0.00	0.12	0.08	0.00	0.09	0.00	0.07	0.03	0.05	0.00	0.05	0.00	0.00	0.01
γ	0.00	0.08	0.07	0.00	0.08	0.00	0.04	0.08	0.00	0.00	0.03	0.07	0.00	0.00	0.00	0.04	0.01	0.00

TABLE 2. Simulation results for SPAT #2 analyzed in absolute mode and in relative mode. All units in millimeters.

	SPAT #2 in absolute mode									SPAT #2 in relative mode								
	Roll test			Pitch test			Yaw test			Roll test			Pitch test			Yaw test		
	X	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*
a	0.01	0.00	0.00	0.01	0.00	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.01	0.00
b	0.00	0.01	0.01	0.00	0.01	0.00	0.01	0.01	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.01	0.00	0.00
c	0.00	0.01	0.01	0.01	0.00	0.01	0.00	0.00	0.01	0.00	0.01	0.00	0.01	0.00	0.00	0.00	0.00	0.00
α	0.00	0.10	0.10	0.00	0.12	0.04	0.00	0.09	0.08	0.00	0.06	0.09	0.00	0.05	0.00	0.00	0.00	0.05
β	0.09	0.07	0.08	0.12	0.00	0.12	0.09	0.00	0.09	0.00	0.07	0.03	0.05	0.00	0.05	0.00	0.00	0.03
γ	0.04	0.09	0.07	0.04	0.09	0.02	0.08	0.09	0.00	0.00	0.03	0.07	0.00	0.00	0.02	0.05	0.03	0.00

The results of the simulations for the two SPATs are shown in Tables 1 and 2. Each of the SPATs are comprised of three tests – a roll test, a pitch test, and a yaw test. Each of these three tests involves probing the nest by rotating the hand held touch probe along one of the three axes. The tables show the *maximum absolute error* in stylus tip along the *X*, *Y*, and *Z* axis for each of these three simulated tests. Each row in the table corresponds to stylus tip error in the presence of an error in one of the six input parameters (a 10 µm error in *a*, *b*, or *c*, or a 1 mrad error in *α*, *β*, or *γ*). The data are analyzed in absolute mode and again in relative mode.

Tables 1 & 2 show that unit errors in the link length reflect as unit errors in one or more of the coordinates; that is, there is no amplification of the errors as expected. Angular errors, however, depend on the Abbe offset and can produce large point coordinate errors. A pitch of 1 mrad, for example, produces a 0.12 mm error along *X* and *Z* for both SPAT configurations in absolute mode for the hand held touch probe under consideration. Those errors drop to 0.05 mm in relative mode, indicating that the relative mode of analysis may attenuate the effect of certain error sources.

There are additional interesting observations that can be made from these tables. A roll test is not necessarily the most sensitive test to detect an error in the roll angle *α*. In fact, the *Y* coordinate in a pitch test is more sensitive to error in the roll angle for the hand held touch probe under consideration. While a pitch test is sensitive to pitch angle errors, yaw angle errors can be captured in any of roll, pitch, or yaw tests. In addition, it can be seen that Tables 1 and 2 are nearly identical indicating that the *Y* offset of 40 mm in SPAT #2 did not produce a noticeable amplification of angular errors in comparison to SPAT #1.

Table 3 shows the experimentally obtained maximum absolute errors along the three axes for the roll, pitch, and yaw test for the two configurations of SPATs. The experiments were repeated three times; the absolute maximum errors from all three repeats are shown in the table. The data for these tests were analyzed in relative mode because the nest used to acquire data was a three-pronged seat for a 6 mm tip that could not seat an SMR. The experimentally observed errors are fairly small, with the largest error on the order of 0.06 mm. It can be seen that the results obtained from simulations (right half of Tables 1 and 2 that show SPAT results based on relative mode of analysis) are also on the order of about 0.07 mm, indicating that the values of input parameters used in the simulations are reasonable. However, as mentioned earlier, we do note that it is possible that the relative mode of analysis has suppressed the effect of certain error sources and therefore the hand held probe may possess error sources that have not been revealed. We plan on performing these tests again in absolute mode in the future.

TABLE 3. Experimentally obtained SPAT errors in millimeters. Data analyzed in relative mode.

	SPAT #1		
	X	Y	Z
Roll test	0.03	0.05	0.02
Pitch test	0.04	0.03	0.03
Yaw test	0.04	0.06	0.06
	SPAT #2		
	X	Y	Z
Roll test	0.03	0.03	0.02
Pitch test	0.04	0.03	0.02
Yaw test	0.03	0.06	0.02

CONCLUSIONS

SPATs are commonly employed to calibrate and evaluate the performance of hand held touch probe accessories of laser trackers. We describe a model based approach to understand the influence of different parameters on stylus tip errors for different configurations of SPATs. As future work, we plan on refining the model and determining more suitable values for input parameters of the simulation, such as better estimates for roll angle errors. We also plan on performing absolute SPATs and length tests along sensitive directions. Characterizing error sources is critical towards developing test procedures that are sensitive to the different error sources.

REFERENCES

[1] R Kupiec, R Dubno, and J Sladek, Accuracy assessment of a laser tracker system, 11th ISMQC, September 11-13 2013, Cracow-Kielce, Poland

[2] K Lau, Y Yang, Y Liu, and H Song, Dynamic performance evaluation of 6D laser tracker sensor, PerMIS'10, September 28-30, 2010, Baltimore, MD

Evaluating IAQ and Energy Impacts of Ventilation in a Net-Zero Energy House Using a Coupled Model

Lisa Ng
William Dols
Dustin Poppendieck
Steven Emmerich

[1]Engineering Laboratory, National Institute of Standards and Technology
100 Bureau Drive Gaithersburg, MD 20899

Content submitted to and published by:
Conference: ASHRAE IAQ 2016 Defining Indoor Air Quality:
Policy, Standards and Best Practices
September 12th- 14th, 2016
Alexandria, VA

U.S. Department of Commerce
Penny Pritzker, Secretary of Commerce

National Institute of Standards and Technology
Willie E May, Director

DISCLAIMERS

Ng, Lisa; Dols, William; Poppendieck, Dustin; Emmerich, Steven.
“Evaluating IAQ and Energy Impacts of Ventilation in a Net-Zero Energy House Using a Coupled Model.”
Paper presented at the 2016 ASHRAE IAQ Conference, Alexandria, VA, Sep 12-Sep 14, 2016.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Any link(s) to website(s) in this document have been provided because they may have information of interest to our readers. NIST does not necessarily endorse the views expressed or the facts presented on these sites. Further, NIST does not endorse any commercial products that may be advertised or available on these sites.

Ng, Lisa; Dols, William; Poppendieck, Dustin; Emmerich, Steven.
“Evaluating IAQ and Energy Impacts of Ventilation in a Net-Zero Energy House Using a Coupled Model.”
Paper presented at the 2016 ASHRAE IAQ Conference, Alexandria, VA, Sep 12-Sep 14, 2016.

Evaluating IAQ and Energy Impacts of Ventilation in a Net-Zero Energy House Using a Coupled Model

Lisa Ng, PhD
Member ASHRAE

Dustin Poppendieck, PhD

W. Stuart Dols
Member ASHRAE

Steven J. Emmerich
Member ASHRAE

ABSTRACT

The National Institute of Standards and Technology (NIST) constructed the Net-Zero Energy Residential Test Facility (NZERTF) to support the development and adoption of cost-effective NZE designs and technologies. Among the key objectives of the facility design was creating a healthy and comfortable environment for the assumed occupants by providing adequate outdoor air ventilation and reducing indoor contaminant sources. Building material source control guidelines were implemented to minimize the use of products with urea-formaldehyde resin and to utilize products with relatively low volatile organic compound (VOC) emissions. Indoor and outdoor concentrations of formaldehyde and acetaldehyde were measured approximately monthly during two years of house operation. Real-time formaldehyde concentration and energy measurements were also used to validate the indoor air quality (IAQ) and energy predictions of a coupled CONTAM-EnergyPlus model of the house. The validated model was then used to evaluate the IAQ and energy impacts of different outdoor air ventilation rates. The results of this work demonstrate the need for appropriate product selection (source control) and mechanical ventilation, especially in homes with relatively airtight envelopes.

INTRODUCTION

Buildings consumed 41 % of all energy used in the United States in 2011, with residential buildings accounting for 22 % (DOE 2011). In addition to consuming more energy than the transportation or industrial sectors, buildings represent the fastest growing sector of energy usage (DOE 2011). Thus, goals for achieving net-zero energy performance have been established in the United States and around the world (City of Melbourne 2014; EPBD 2010; IEA 2014). A net-zero energy building (ZEB) is an energy-efficient building where, on a source energy basis, the actual annual delivered energy is less than or equal to the on-site renewable exported energy (DOE 2015a).

The Net-Zero Energy Residential Test Facility (NZERTF) was constructed at the National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland to support the development and adoption of cost-effective net-zero energy (NZE) designs, technologies, and construction methods. The two-story house shown in Figure 1 has a basement and attic, and is similar in size (242 m^2 of occupied floor area, with 485 m^2 inside the building envelope including the attic and basement) and aesthetics to homes in the surrounding communities. The house is unoccupied and not furnished other than permanently installed cabinetry.

Many technologies are employed in the house to achieve the NZE goals including a 10.2 kW photovoltaic (PV) system, a high efficiency air-to-air heat pump, a solar hot water system, and a heat recovery ventilator (HRV). All floors of the house, including the attic, are within the conditioned space. A central heat pump system provides supply air to all

Ng, Lisa; Dols, William; Poppendieck, Dustin; Emmerich, Steven.
"Evaluating IAQ and Energy Impacts of Ventilation in a Net-Zero Energy House Using a Coupled Model."
Paper presented at the 2016 ASHRAE IAQ Conference, Alexandria, VA, Sep 12-Sep 14, 2016.

floors except the attic. Passive air transfer grilles connect the basement to the first floor and attic to the second floor of the house. Air is returned to the heat pump via three return air grilles located on the first and second floors. A balanced and ducted HRV system supplies outdoor air to the first floor kitchen and second floor bedrooms, while drawing air for heat recovery from one bathroom located on the first floor and two on the second floor. To comply with the minimum ventilation requirements in the ASHRAE Standard 62.2-2010 (ASHRAE 2010), the HRV was sized to deliver 137 m^3 h^{-1} of outdoor air, but actually delivered 171 m^3 h^{-1} based on the available fan speeds in the unit. This rate did not include any infiltration credit. More information on the NZERTF design can be found in Pettit et al. (2014).

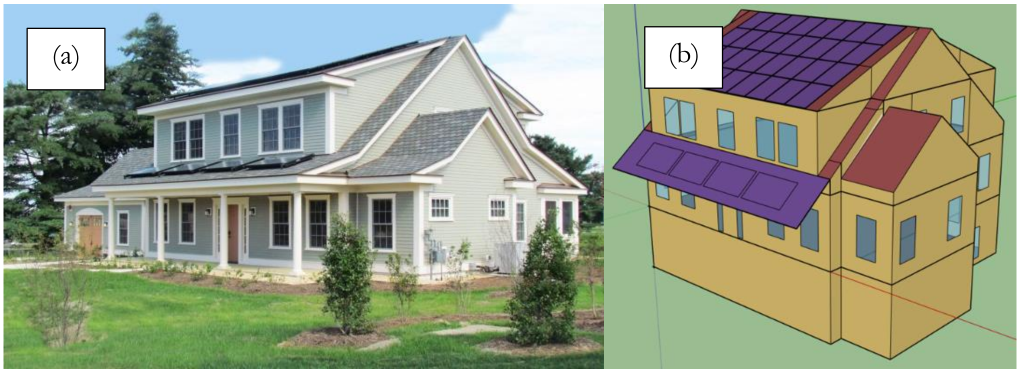


Figure 1 (a) Photograph of NZERTF and (b) Three-dimensional representation of NZERTF EnergyPlus Model

The pursuit of net-zero energy is often done with little or no verification of the achievement of acceptable indoor air quality (IAQ). Teichman et al. (2015) reviewed 100 cases studies of high performance buildings and found 60 implemented source control by using low-VOC (volatile organic compounds) emitting materials but generally provided little information on the specifics supporting these claims. Only two of the case studies measured actual chemical concentrations in the building. Concentration verification is a vital step in buildings with low air change rates, as low-VOC emitting building materials can still result in elevated concentrations if building air change rates are not adequate or if chemicals are emitted that are not captured in the emissions testing.

The NZERTF was built minimizing use of products with urea-formaldehyde resin and with products that had low emissions of VOC. The guidelines for the building product selection and construction best practices for IAQ used at the NZERTF are available as architectural specifications in Bernheim and Hodgson (2014). After construction of the home, indoor and outdoor concentrations of formaldehyde and 30 other VOCs were measured approximately monthly during two years of house operation, and the results reported in Poppendieck et al. (2015). Formaldehyde emission factors in the NZERTF are on average at least four times lower than comparable houses. However, NZERTF concentrations of some VOCs are higher than comparable houses with 20 % higher air change rates (Ullah et al. 2016).

According to the International Agency for Research on Cancer (IARC), formaldehyde is a human carcinogen (IARC 2006) and acetaldehyde is a probable human carcinogen (IARC 1999). The EPA does not define any acceptable exposure levels to carcinogens but does define unit risk factors to estimate inhalation cancer risk from chronic exposure to a chemical. A user can define the acceptable risk level and use the unit risk factor to determine the chemical concentration equivalent to that acceptable risk level. In this study, risk levels of 1 cancer in 1 000 000 people (10^{-6}) and 1 cancer in 10 000 people (10^{-4}) from exposure to formaldehyde and acetaldehyde were evaluated, which are lower and upper risk levels that have been used by the EPA for air toxics in outdoor air (EPA 1999).

In addition to cancer effects, both formaldehyde and acetaldehyde can have chronic harmful (i.e., deleterious) noncancerous impacts, including for example eye, nose or throat irritation. California Office of Environmental Health Hazard Assessment (OEHHA) chronic relative exposure level (cREL) and the EPA inhalation reference concentration (RfC) are both concentrations below which there are deemed to be no deleterious noncancerous impacts. These values are also summarized in Table 1.

To better understand the impact of product selection (i.e., contaminant emission rates) and outdoor air ventilation rates on building energy use and IAQ, a coupled thermal-airflow model of the house was developed. The model was validated using measured energy use and real-time formaldehyde concentration measurements. The validated model was then used to simulate the energy use and indoor concentrations of formaldehyde and acetaldehyde for different outdoor air ventilation rates.

Table 1. Summary of Health References

Contaminant	IARC Designation	Agency/Reference	Type	Concentration
Acetaldehyde	Probable Human Carcinogen	EPA (1988)	1 in 1 000 000 cancer risk	0.5 μg m^{-3}
		EPA (1988)	1 in 10 000 cancer risk	50 μg m^{-3}
		EPA (2000)	RfC	9 μg m^{-3}
		OEHHA (2016)	cREL	140 μg m^{-3}
Formaldehyde	Human Carcinogen	EPA (1989)	1 in 1 000 000 cancer risk	0.08 μg m^{-3}
		EPA (1989)	1 in 10 000 cancer risk	8 μg m^{-3}
		OEHHA (2016)	cREL	9 μg m^{-3}

SIMULATION MODEL

Modelling of the NZERTF was performed using the whole-building multizone airflow and indoor air quality software CONTAM (Dols et al. 2015) coupled with EnergyPlus, a whole-building energy analysis software (DOE 2015b). CONTAM accounts for the interaction between external driving forces (ambient temperature and wind) and internal mechanisms (building heating, ventilating, and air-conditioning (HVAC) system airflows) to determine resultant pressures and airflows across internal and external building partitions, i.e., interzone airflows and infiltration/exfiltration rates. CONTAM can also account for external and internal contaminant sources and removal mechanisms to calculate contaminant transport associated with the previously determined airflows. EnergyPlus implements a multizone heat transfer model that accounts for conductive, convective and radiant heat transfer associated with building materials (e.g., walls, floors, ceilings and windows); interzone and infiltration airflows; and HVAC systems. CONTAM requires the user to define zone air temperatures while EnergyPlus requires the user to input infiltration and interzone airflow rates. Recent enhancements to both programs enable run-time coupling between them in a quasi-dynamic manner (Dols et al. 2016; Wetter 2011). During coupled simulations, indoor temperatures and HVAC system flow rates are passed from EnergyPlus to CONTAM, and airflow rates across the building envelope and between internal zones are passed from CONTAM to EnergyPlus. These coupled simulations thereby account for wind-driven, stack-driven and ventilation system driven infiltration and ventilation rates based upon measurements of actual envelope leakage characteristics and HVAC system airflow rates.

The NZERTF was modelled as a five zone building consisting of one zone for each floor and two attic spaces, a main one above the second floor and a smaller one above the living room on the east side (see Figure 1). Model inputs were determined based on building design information and measurements as follows. Ventilation system airflow rates were measured; including heat pump supply and return, HRV supply and return, range hood, and dryer vent exhaust. Average measured rates were input into the CONTAM-EnergyPlus model. Emission rates in this study are effective emission rates that combine emission and removal mechanisms. The average effective, occupied floor area (1st floor and 2nd floor) formaldehyde emission rate over one year (6.7 μg h^{-1} m^{-2}) was measured using one hour 2,4-dinitrophenylhydrazine (DNPH) cartridge sampling according to ASTM D5197 (ASTM 2009) and was reported in Poppendieck et al. (2015). The effective emission rate accounts for both sources and sinks in the NZERTF. Previous investigations indicated that there was likely no significant source of formaldehyde in the basement, but there are likely sources on other levels. The formaldehyde source was modeled as being present on the 1st, 2nd and attic floors. Hence, the effective floor area formaldehyde emission rate was normalized to include the attic floor area and modeled as 5.1 μg h^{-1} m^{-2} in this study. The average effective acetaldehyde emission rate was normalized and modeled over the basement, 1st, 2nd, and attic floors (7.4 μg h^{-1} m^{-2}). It was assumed that the outside concentration of formaldehyde and acetaldehyde were both 0.0 μg m^{-3} in the model, though measured outdoor formaldehyde and acetaldehyde concentrations were both on average 0.8 μg m^{-3} between November 2013 and March 2014 based on periodic measurements (Poppendieck et al. 2015). All model inputs are listed in Table 2.

Table 2. Summary of Inputs in Coupled CONTAM-EnergyPlus Model of NZERTF

Input	Value
Heat pump max airflow	1500 m^3 h^{-1}
HRV average supply and exhaust airflow	171 m^3 h^{-1}
Kitchen range hood airflow	180 m^3 h^{-1}
Dryer exhaust airflow	60 m^3 h^{-1}
Building envelope airtightness	0.37 cm^2 m^{-2} at 4 Pa
Formaldehyde emission	5.1 μg h^{-1} m^{-2}
Acetaldehyde emission	7.4 μg h^{-1} m^{-2}

Blower door tests were performed to measure the building envelope leakage rate with the HRV outside air and exhaust vents sealed. The building envelope leakage rate was 803 m^3 h^{-1} at 50 Pa (Ng et al. 2015). In the CONTAM model, this envelope leakage was distributed uniformly over the entire above-grade building envelope with an effective leakage area of 0.37 cm^2 m^{-2} at 4 Pa. Details of this conversion can be found in the ASHRAE (2013).

The EnergyPlus model, including all of the systems and internal loads, was developed and validated with measured electrical and water-use data by Kneifel et al. (2015). This EnergyPlus model was then used to develop the EnergyPlus representation of the coupled CONTAM-EnergyPlus model used in this study.

An Actual Meteorological Year (AMY) weather file from July 2013 to June 2014 for the Montgomery County Airpark (KGAI) weather station (Weather Analytics 2014), located about 11 km from the NIST campus, was used in the simulations. The simulated annual heating, cooling, and total energy use predicted by the coupled CONTAM-EnergyPlus model are shown in Figure 2, along with the measured energy use (Fanney et al. 2015). The simulated annual house energy consumption (13 600 kWh) was 5 % more than the measured energy consumption (12 900 kWh). The simulated annual PV production (14 400 kWh) was 6 % more than the measured PV production (13 500 kWh).

Model Validation

Measurements from a real-time spectrophotometric formaldehyde monitor, which were taken approximately one year after the Poppendieck et al. (2015) measurements, were used to validate the coupled model. The sensitivity of the monitor is 0.12 μg m^{-3} with a one second sampling time. Sampling tubes were run from the basement, living room, master bedroom, and attic to an automatic seven port sampling valve having a common port to the monitor. Detailed discussion on the real-time formaldehyde measurements can be found in Poppendieck et al. (2016).

The real-time formaldehyde measurements were taken with the HRV operating for 40 minutes out of every hour at 205 m^3 h^{-1}, yielding an average hourly outdoor air ventilation rate of 137 m^3 h^{-1} (which corresponds to the ASHRAE 62.2-2010 minimum required ventilation rate for the house). In contrast, the HRV ran continuously at 171 m^3 h^{-1} during the measurement of formaldehyde concentrations used to calculate the emission rates in the coupled model. The simulated and measured concentrations are shown in Figure 3. The simulated and measured formaldehyde concentrations follow similar trends and are of the same magnitude in all of the zones. The average measured and simulated formaldehyde concentrations in the basement, first, and second floors was 7.9 μg m^{-3} (standard deviation=0.9 μg m^{-3}) and 8.3 μg m^{-3} (standard deviation=0.2 μg m^{-3}), respectively. The average measured and simulated formaldehyde concentrations in the attic were 22.2 μg m^{-3} (standard deviation=2.3 μg m^{-3}) and 19.5 μg m^{-3} (standard deviation=2.0 μg m^{-3}), respectively. With the coupled model validated with real-time formaldehyde measurements, different outdoor air ventilation rates were simulated to observe the effects on indoor concentrations and energy use.

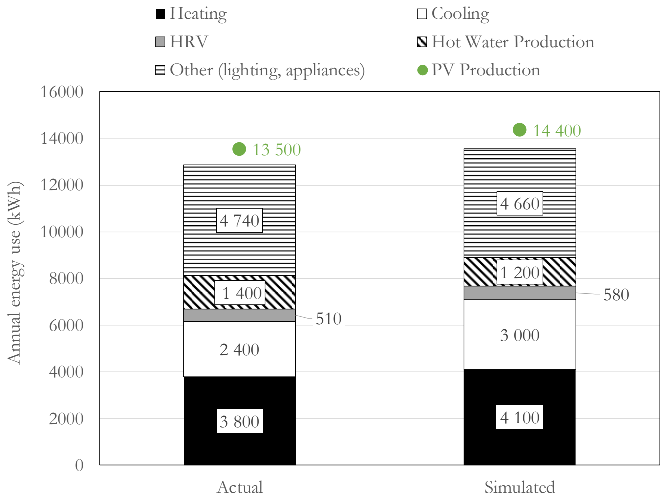


Figure 2 Comparison of actual and simulated annual energy use and PV production

Simulations

The following outdoor air ventilation rates were simulated: HRV off, 171 m^3 h^{-1} (NZERTF ventilation rate), 137 m^3 h^{-1} (ASHRAE Standard 62.2-2010 minimum requirement), 280 m^3 h^{-1} (ASHRAE 62.2-2013 minimum requirement), and a rate to bring both formaldehyde and acetaldehyde below nondeleterious, noncancerous benchmarks (RfC and cREL values in Table 1). Simulations were performed using an AMY weather file for the KGAI weather station for July 2013 to July 2014 (Weather Analytics 2014). The modeled HRV fan power was increased in proportion to the increase in airflow rate from the NZERTF ventilation rate, but no other changes to the performance parameters were made. The IAQ and energy use consequences of the five outdoor air ventilation rates were compared.

RESULTS AND DISCUSSION

The simulated annual average formaldehyde and acetaldehyde concentrations, calculated for the 1st and 2nd floors, for the five outdoor air ventilation scenarios as a function of the total simulated energy use are shown in Figure 4. The acetaldehyde and formaldehyde health references are shown as horizontal red lines. The simulated annual energy use for net-zero operation (14 400 kWh) is shown as a dotted vertical green line.

Formaldehyde. Despite source control measures to minimize the use of building products with urea-formaldehyde resin, none of the simulated ventilation rates reduced concentrations below the concentration associated with a cancer risk of 1 in 1 000 000 (0.08 μg m^{-3}). The outside concentration of formaldehyde measured at the NZERTF was also above this concentration. The simulated NZERTF annual average formaldehyde concentration of 7.1 μg m^{-3} was lower than the formaldehyde concentration associated with a cancer risk of 1 in 10 000 (8.0 μg m^{-3}) and the OEHHA cREL (9.0 μg m^{-3}). The simulated concentration was also lower than 13 newly constructed, occupied homes designed to meet EPA Indoor airPlus guidelines (Hult et al. 2015), and all but two of 108 occupied, new standard construction homes in California (Offermann 2009). The average outdoor ventilation rate measured in the homes in the Hult study was 0.26 h^{-1}, which is equivalent to 330 m^3 h^{-1} in the NZERTF and is almost twice the ventilation rate of the NZERTF. The average outdoor ventilation rate measured in the Offermann study was 0.24 h^{-1}, which is equivalent to 305 m^3 h^{-1} in the NZERTF and a little more than 1.5 times more than the NZERTF ventilation rate. At a 25 % lower outdoor air ventilation rate, the ASHRAE 62.2-2010 rate of 137 m^3 h^{-1}, the simulated annual average concentration of formaldehyde increased 17 % to 8.5 μg m^{-3}. When accounting for the measured average outdoor formaldehyde concentration, the ASHRAE 62.2-2010 ventilation rate results in a concentration that is above both the concentration associated with a cancer risk of 1 in 10 000 (8.0 µg m^{-3}) and the OEHHA cREL (9.0 µg m^{-3}). The simulated annual energy savings would be 4 % when ventilating 25 % less using the KGAI AMY weather file.

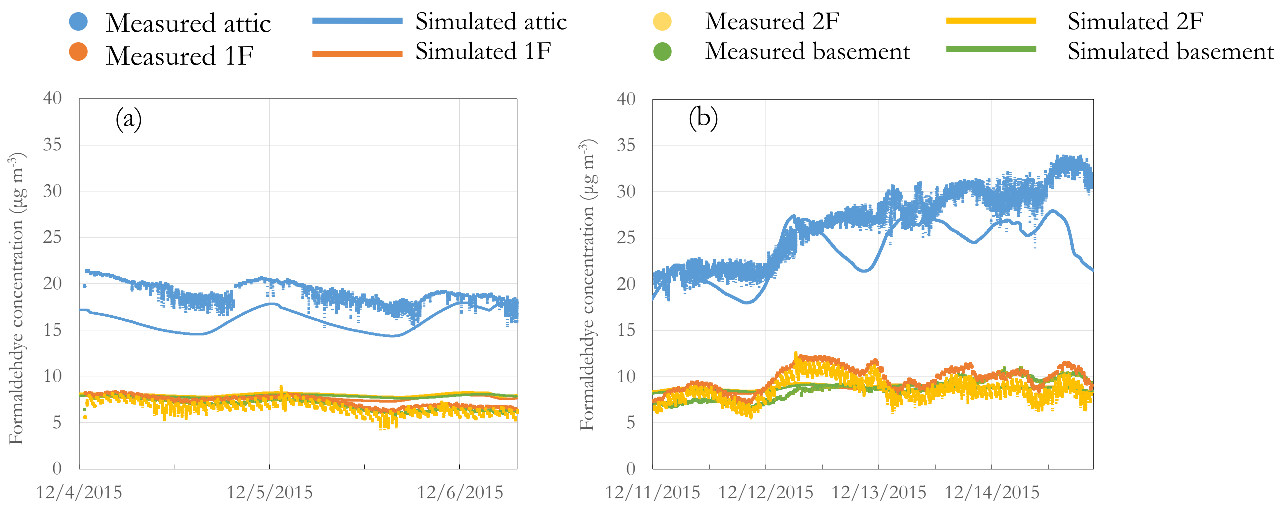


Figure 3 Real-time formaldehyde concentration data from two sampling sessions. (a) Average outdoor temperature was 3.5 °C (b) Average outdoor temperature was 12.7 °C. Average wind speed (both sessions) was 0.9 m s^{-1}

Acetaldehyde. While low emission building products were specified for the construction of the NZERTF, acetaldehyde was not specifically targeted. Like formaldehyde, none of the simulated ventilation rates reduced acetaldehyde concentrations below the concentration associated with a cancer risk of 1 in 1 000 000 (0.5 µg m^{-3}). At the NZERTF outdoor air ventilation rate, the simulated annual average acetaldehyde concentration was 15.7 µg m^{-3}, which is below the concentration associated with a cancer risk of 1 in 10 000 (50 µg m^{-3}) and the OEHHA cREL (140 µg m^{-3}) but above the EPA RfC (9.0 µg m^{-3}). Roughly 35 % of the 108 California homes had acetaldehyde concentrations lower than the EPA RfC value (Offermann 2009). The outdoor air ventilation rate required to bring the levels of acetaldehyde concentrations below the EPA RfC would be at least the ASHRAE 62.2-2013 rate of 280 m^3 h^{-1} with an associated energy increase of at least 13 % using the KGAI AMY weather file. At this ventilation rate, the model predicts the house would no longer achieve net-zero energy use for the year as operated, i.e. heating and cooling with an air-to-air heat pump and ventilating continuously. Without any mechanical outdoor air ventilation, the indoor concentrations of formaldehyde and acetaldehyde would be almost 85 % higher with an associated 20 % reduction in annual energy use.

This study demonstrates the need for source control in homes with relatively airtight envelopes. At the NZERTF, controlling for formaldehyde emissions was a key design objective, leading to concentrations roughly four times less than in other new homes. However, the NZERTF was unfurnished, unoccupied, and occupied only on occasion for maintenance or tours. Hence, the data presented in Figure 4 only accounts for the emissions attributed to the building materials. Occupants in real homes will likely introduce formaldehyde and acetaldehyde through furniture and secondary ozone reactions with household products, personal care products and secondary reactions with their own skin oils (Salthammer et al. 2010). Hence, contaminant modeling of building product emissions should only be used a starting point when designing or setting ventilation rates.

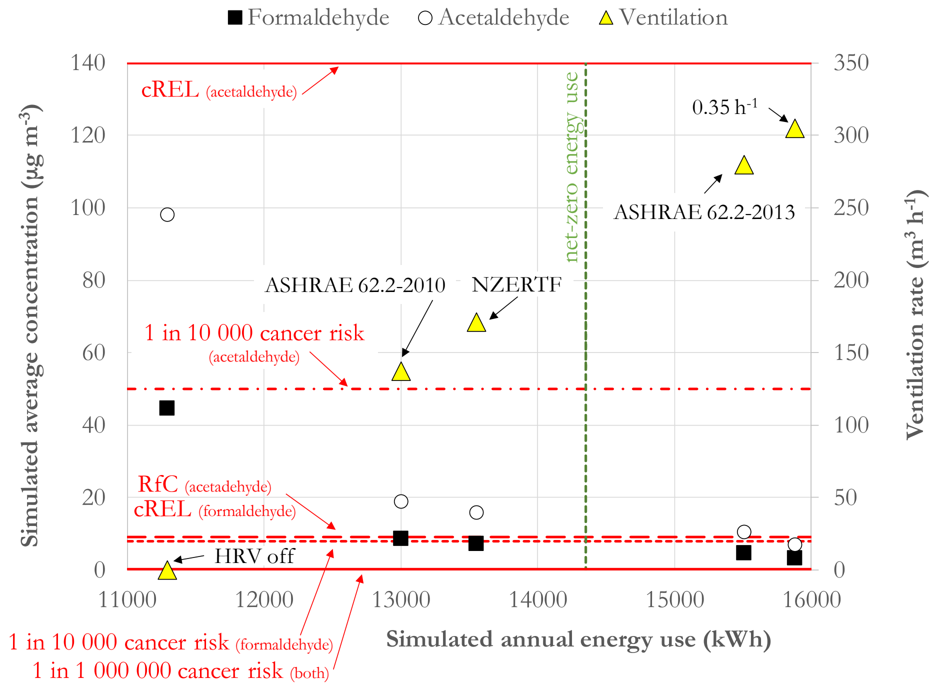


Figure 4 Simulated annual average formaldehyde and acetaldehyde concentrations for five ventilation rates and their associated simulated annual energy consumption

CONCLUSION

The NIST NZERTF was constructed to support the development and adoption of cost-effective NZE designs and technologies, and to demonstrate that net-zero could be achieved while meeting the needs and comfort of occupants. To support these objectives, building material source control guidelines were implemented to minimize the use of products with urea-formaldehyde resin and to utilize products with relatively low VOC emissions. Indoor and outdoor measurements of formaldehyde and acetaldehyde were used to calculate emission rates that were input into a coupled CONTAM-EnergyPlus model of the house to verify that these design goals were met. The model was also used to study the effect of lower and higher outdoor air ventilation rates on the indoor concentrations of formaldehyde and acetaldehyde and on annual energy use. None of the ventilation rates reduced formaldehyde and acetaldehyde concentrations below the concentrations associated with a cancer risk of 1 in 1 000 000, the lower risk level used by the EPA for air toxics in outdoor air. In contrast, all simulated ventilation rates at or greater than the existing NZERTF rate would result in acetaldehyde and formaldehyde concentrations lower than those associated with a cancer risk of 1 in 10 000. The NZERTF could be operated at a 25 % lower ventilation rate (4 % energy savings) and still meet the OEHHA cREL of 9 µg m^{-3} for formaldehyde, which is a health benchmark below which there are deemed to be no deleterious noncancerous impacts. However, to prevent nondeleterious, noncarcinogenic effects from acetaldehyde exposure (EPA RfC of 9 µg m^{-3}), the building outdoor air ventilation rate would have to increase more than 39 %, with an associated annual energy increase of more than 13 %. At this rate, the NZERTF, as currently operated, would no longer achieve net-zero operation given the weather conditions of the year modeled. This study demonstrates that selecting appropriate outdoor air ventilation rates for a residence can be complex. Lower outdoor air ventilation rates can lead to lower energy use but result in increased levels of indoor contaminants. Increasing the outdoor air ventilation rate to meet health benchmarks is also not straightforward. If the IAQ design target is to prevent deleterious, noncarcinogenic chronic effects, increased outdoor air ventilation rates may be needed but could come at the cost of net-zero energy operation. An IAQ design target of an acceptable cancer risk of 1 in 1 000 000 may be difficult to achieve for some chemicals, such as formaldehyde, with any reasonable ventilation rate, especially if the outdoor concentration of the contaminant is already higher than this level. An IAQ design target of an acceptable cancer risk of 1 in 10 000 may be achievable from a ventilation standpoint, but poses a greater potential carcinogenic risk to the occupants.

REFERENCES

Bernheim, A., P. White and A. Hodgson 2014. High Performance Indoor Air Quality specification for Net Zero Energy Homes. *NIST GCR 14-980*. Gaithersburg, MD: National Institute of Standards and Technology.

City of Melbourne (2014). Zero Net Emissions by 2020. Melbourne, Australia: City of Melbourne.

DOE 2011. Building Energy Data Book.

DOE 2015a. A Common Definition for Zero Energy Buildings. Washington, D. C.: U. S. Department of Energy.

DOE 2015b. EnergyPlus 8.4.

Dols, W.S., S.J. Emmerich and B.J. Polidoro 2016. Coupling the multizone airflow and contaminant transport software CONTAM with EnergyPlus using co-simulation. *Building Simulation* (9):469-479.

Dols, W.S. and B. Polidoro 2015. CONTAM User Guide and Program Documentation. *NISTIR 7251*. Gaithersburg, MD: National Institute of Standards and Technology.

EPA (1988). Integrated Risk Information System (IRIS) – Acetaldehyde.

EPA (1989). Integrated Risk Information System (IRIS) – Formaldehyde.

EPA (1999). RESIDUAL RISK: Report to Congress. Research Triangle Park, NC: U. S. Environmental Protection Agency: Office of Air Quality Planning and Standards. EPA-453/R-99-001.

EPA (2000). Air Toxics Web Site - Acetaldehyde from https://www3.epa.gov/airtoxics/hlthef/acetalde.html.

EPBD (2010). Energy Performance of Buildings Directive. Brussels, Belgium.

Fanney, A.H., V. Payne, T. Ullah, L. Ng, M. Boyd, F. Omar, M. Davis, H. Skye, B. Dougherty, B. Polidoro, W. Healy, J. Kneifel and B. Pettit 2015. Net-zero and beyond! Design and performance of NIST's net-zero energy residential test facility. *Energy and Buildings* 101(0):95-109.

Hult, E.L., H. Willem, P.N. Price, T. Hotchi, M.L. Russell and B.C. Singer 2015. Formaldehyde and acetaldehyde exposure mitigation in US residences: In-home measurements of ventilation control and source control. *Indoor Air* 25.

IARC (1999). IARC Monographs on the Evaluation of Carcinogenic Risks to Humans: Re-Evaluation of Some Organic Chemicals, Hydrazine and Hydrogen Peroxide. Lyon, France: International Agency for Research on Cancer.

IARC (2006). IARC Monographs on the Evaluation of Carcinogenic Risks to Humans: Formaldehyde, 2-Butoxyethanol and 1-tert-Butoxypropan-2-ol. Lyon, France: International Agency for Research on Cancer.

IEA (2014). Regional Energy Efficiency Policy Recommendations: Southeast Asia Region. Paris, France: International Energy Agency.

Kneifel, J., V. Payne, T. Ullah and L. Ng 2015. Simulated versus Measured Energy Performance of the NIST Net Zero Energy Residential Test Facility Design. *NIST Special Publication 1182*. Gaithersburg, MD: National Institute of Standards and Technology.

Ng, L., A. Persily and S. Emmerich 2015. Infiltration and Ventilation in a Very Tight, High Performance Home. *36th AIVC Conference Effective Ventilation in High Performance Buildings*. Madrid, Spain.

OEHHA (2016). OEHHA Acute, 8-hour and Chronic Reference Exposure Level (REL) Summary from http://oehha.ca.gov/air/general-info/oehha-acute-8-hour-and-chronic-reference-exposure-level-rel-summary.

Offermann, F.J. 2009. Ventilation and Indoor Air Quality in New Homes. California Air Resources Board and California Energy Commission.

Pettit, B., C. Gates, A.H. Fanney and W. Healy 2014. Design Challenges of the NIST Net Zero Energy Residential Test Facility. *NIST TN-1847*. Gaithersburg, MD: National Institute of Standards and Technology.

Poppendieck, D., S. Khurshid, W.S. Dols, L. Ng, B. Polidoro and S. Emmerich 2016. Formaldehyde Concentrations in a Net-Zero Energy House: Real-time Monitoring and Simulation. *Proceedings of Indoor Air 2016*. Ghent, Belgium.

Poppendieck, D.G., L.C. Ng, A.K. Persily and A.T. Hodgson 2015. Long Term Air Quality Monitoring in a Net-Zero Energy Residence Designed with Low Emitting Interior Products. *Building and Environment* 94(1):33-42.

Salthammer, T., S. Mentese and R. Marutzky 2010. Formaldehyde in the Indoor Environment. *Chemical Reviews* 110(4):2536-72.

Teichman, K.Y., A.K. Persily and S.J. Emmerich 2015. Indoor air quality in high-performing building case studies: Got data? *Science and Technology for the Built Environment* 21(1):91-98.

Ullah, T., D. Poppendieck, W.M. Healy, A.H. Fanney and K.Y. Teichman 2016. Energy and Indoor Air Quality Benchmarking of the NIST Net-Zero Energy Residential Test Facility (NZERTF). *2016 ACEEE Summer Study on Energy Efficiency in Buildings*. Pacific Grove, CA. *Publication pending*.

Weather Analytics 2014. Actual Meteorological Year (AMY) formatted weather data for July 1, 2013 through June 30, 2014.

Wetter, M. 2011. Co-simulation of building energy and control systems with the Building Controls Virtual Test Bed. *Journal of Building Performance Simulation* 4(3):185-203.

ECS Transactions, 72 (3) 113-117 (2016)
10.1149/07203.0113ecst ©The Electrochemical Society

Hardware Security to Mitigate Threats to Networked More-Than-Moore Sensors [#]

Yaw Obeng
Engineering Physics Group, Physical Measurement Laboratory, Nation Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899

Author's Contact Information: Email: yaw.obeng@nist.gov Phone: 301-975-8093

[#]Official contribution of the National Institute of Standards and Technology; not subject to copyright in the United States.

Keywords: security ; design ; emerging technology ; hardware security;

Abstract: Networked sensors (a. k. a., Internet of Things (IoT)) represents a new era in the evolution of telecommunications made possible by the reduced cost of performance in electronic devices. This is the era where even the most mundane items are connected to, and communicate with each other, on massive networks. This paper examines the issues pertaining to, and efforts at improving, the hardware security of the interconnected devices. The paper highlights a number of academia and semiconductor industry-led ongoing work on improving hardware security.

The Internet of Things (IoT) represents a new era in the evolution of telecommunications, made possible by the reduced cost of performance in electronic devices. Even the most mundane items are communicating with each other through a network of sensors made possible because of the convergence of wireless technologies, advancements of microelectromechanical systems (MEMS) and digital electronics, i.e. More-than Moore technologies. The net result is an emerging system comprised of many small, inexpensive single-function devices, with varying operating systems, CPU types, memory, etc. How these devices connect to each other, and to humans, are changing how we work and live. Unfortunately, the weaknesses of the underlying networks have been exposed through exploitations of hardware operation weaknesses(1). By and large, unsecured smart devices threaten the convenience of the More-than-Moore technology platforms. Thus, security must be the foundational enabler for such technologies; without ample security measures, the ever expanding sensor network could create massive vulnerabilities. Hardware security is a critical component of the security envelope. Major threats from hardware vulnerabilities could also invalidate software-centric cybersecurity solutions. Implementing security improvements at the hardware level through design changes generally tends to be very efficient than after deployment fixes, and can enable higher level function in some cases.

There have been a number of academia-led efforts to leverage unique current-voltage (I-V) characteristics associated with beyond-CMOS transistors to design novel security primitives into emerging devices. For example, the inherent ambipolarity of some nanoscale devices can be leveraged to deliberately change device characteristics post-deployment(2-4). In symmetric graphene FETs (SymFET)-like devices, it is conceptually possible to create polymorphic

Downloaded on 2016-09-07 to IP 129.6.65.30 address. Redistribution subject to ECS terms of use (see ecsdl.org/site/terms_use) unless CC License in place (see abstract).

electronics, with multiple functionalities built into the same cell(5-7). Polymorphic gates can conceal the functionality of a digital circuit even if the adversary has access to an entire netlist (8). SymFET-based “protector circuits’’ have been developed to help prevent power supply fault injections(8). In another example, the unique electronic properties of resistive RAMs (and memristors) have been used to perform lightweight user authentication in units that are secure and reliable against environmental variations such as temperature, noise, unbalanced set/reset, filament formation variation and device aging(9). There are other device concepts and primitives, such as those based on negative capacitance FETs, that can lead to improved hardware security(10). In all these examples, new and emerging materials provide the unique properties and phenomena that make these circuits possible.

In addition to device design changes and IP security, manufacturing and supply chain security, and product traceability offer opportunities to improve network security. The increased sophistication of counterfeiters has made it more difficult to detect counterfeit products and to verify the presence of malicious content in electronic products. Since the entire integrated circuit (IC) design flow, manufacturing and application phases are currently distributed world-wide, there is a need to authenticate products against malicious products in the supply chain. The diffused supply chains of the manufacturing process increase the complexity of verifying products and materials authenticity. This requires hardware authentication solutions based on standards that can be easily implemented across the supply chain. It must be implemented and supported throughout the entire manufacturing supply chain, comprising raw material providers, parts suppliers, end-item manufacturers, system integrators, shippers, border crossings, seaports, truck inspection and weigh stations, distributors, maintenance service providers, retailers, and consumers, etc. There are several product authentication technologies in the marketplace, but for these to be useful they should provide a level of security against consumer deception where the legitimacy of the product materials and components ensure it does not impose additional hazards in terms of security or safety.

Detecting counterfeit products, especially ICs, may be extremely difficult if not impossible even if comprehensive functional tests are used. The IC may respond as designed to applied stimulus signals, however, the circuit may have additional malicious functions added for the purposes of intentionally inducing malfunctions or a “back door” for extracting secure information. Also, counterfeit ICs may be manufactured with a marginal fabrication process where the reliability of the product may be severely compromised causing the product to fail unexpectedly. Such a failure would be devastating in critical applications such as medical implants, automotive control systems, military, or aerospace. Thus, testing and measurement techniques will need to be developed and continuously improved for the detection of counterfeit or malicious content as the attacks gain sophistication.

Downloaded on 2016-09-07 to IP 129.6.65.30 address. Redistribution subject to ECS terms of use (see ecsdl.org/site/terms_use) unless CC License in place (see abstract).

The following are illustrative examples of industry-lead efforts towards addressing the aforementioned issues. The Open Interconnect Consortium (OIC) sponsored open source software framework enabling seamless device-to-device connectivity. In a different effort, the High Density Packaging User Group (HDPUG) has evaluated most of the hardware authentication technologies currently available, and determined the best known methods and examples for each technology(11). iNEMI has surveyed the possible points of entry of counterfeit components in the supply chain and assessed the impact on the industry at various points of use. They have also developed a set of risk assessment calculators that can be used to quantify the risks of procuring counterfeit parts(12). SEMI has developed and published a number of technical standards to help deter counterfeiting by validating the integrity of goods at the point of purchase. The SEMI T20 and its associated subsidiary standards describe: the overall system, object labeling, authentication service communication, and authentication service body (ASB) qualifications to enable data exchange(13). Finally, the Open group has created an open standard containing a set of organizational guidelines, requirements, and recommendations for integrators, providers, and component suppliers to enhance the security of the global supply chain and the integrity of electronic products. If properly adhered, the open standard will help assure against maliciously tainted and counterfeit products throughout the product life cycle including: design, sourcing, build, fulfillment, distribution, sustainment, and disposal(14).

The semiconductor industry has also identified the need for a concerted effort to provide non-hardware solutions to the identified networked hardware security issues. Suggestions include a cyber-security management (CSM) system that will enable organizations to develop, deploy, and scale secure applications and online services. The CSM will also help manage digital identities, and automate and centralize the management of digital certificates. Such a system should be scalable, interoperable, easily deployed and administered. The standards development must be holistic and should encompass hardware, software and network.

Conclusions

Hardware security and privacy are becoming a critical design consideration, just like performance, power, and reliability, etc. These critical issues must be tackled in part by mitigating counterfeit components entering the supply chain, and onto the internet. The good news is that there many, albeit disparate, industry-lead efforts towards securing the supply chain but these efforts can be better coordinated to provide a more holistic solution to the problem. These requirements are best managed based upon industry-led standards that can be easily implemented across the supply chain. Also, research must be conducted to identify potential technical solutions to provide enhanced hardware security features.

Downloaded on 2016-09-07 to IP 129.6.65.30 address. Redistribution subject to ECS terms of use (see ecsdl.org/site/terms_use) unless CC License in place (see abstract).

References

1. Greenberg A. Hackers Remotely Kill a Jeep on the Highway—With Me in It http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ 2015 [cited 2016 February, 19]. Blog].
2. Colli A, Pisana S, Fasoli A, Robertson J, Ferrari AC. Electronic transport in ambipolar silicon nanowires. physica status solidi (b). 2007;244(11):4161-4.
3. Martel R, Derycke V, Lavoie C, Appenzeller J, Chan KK, Tersoff J, et al. Ambipolar Electrical Transport in Semiconducting Single-Wall Carbon Nanotubes. Physical Review Letters. 2001;87(25):256805.
4. Seabaugh AC, Qin Z. Low-Voltage Tunnel Transistors for Beyond CMOS Logic. Proceedings of the IEEE. 2010;98(12):2095-110.
5. Stoica A, Zebulum RS, Guo X, Keymeulen D, Ferguson MI, Duong V. Taking evolutionary circuit design from experimentation to implementation: some useful techniques and a silicon demonstration. IEE Proceedings - Computers and Digital Techniques [Internet]. 2004; 151(4):[295-300 pp.]. Available from: http://digital-library.theiet.org/content/journals/10.1049/ip-cdt_20040503.
6. Pei Z, Feenstra RM, Gong G, Jena D. SymFET: A Proposed Symmetric Graphene Tunneling Field-Effect Transistor. Electron Devices, IEEE Transactions on. 2013;60(3):951-7.
7. Fallahazad B, Lee K, Kang S, Xue J, Larentis S, Corbet C, et al. Gate-Tunable Resonant Tunneling in Double Bilayer Graphene Heterostructures. Nano Letters. 2015;15(1):428-33.
8. Yu B, Gaillardon PE, Hu XS, Niemier M, Jiann-Shiun Y, Yier J, editors. Leveraging Emerging Technology for Hardware Security - Case Study on Silicon Nanowire FETs and Graphene SymFETs. Test Symposium (ATS), 2014 IEEE 23rd Asian; 2014 16-19 Nov. 2014.
9. Arafin MT, Qu G. RRAM Based Lightweight User Authentication. Proceedings of the IEEE/ACM International Conference on Computer-Aided Design; Austin, TX, USA. 2840839: IEEE Press; 2015. p. 139-45.
10. Kobayashi M, Hiramoto T, editors. Device design guideline for steep slope ferroelectric FET using negative capacitance in sub-0.2V operation: Operation speed, material requirement and energy efficiency. VLSI Technology (VLSI Technology), 2015 Symposium on; 2015 16-18 June 2015.
11. Obeng YS. "Evaluation Of Product Authentication Technologies: A Detailed Evaluation Of The Current And Emerging Technologies", Obeng, Y. et al, presented at S College Park, MD: MTA / CALCE Symposium on Counterfeit Parts and Materials, Technical Symposium and Expo: June 23-24, 2015, ; 2015 [February 22, 2016]. Available from: http://www.calce.umd.edu/symposiums/SCEPJune2015_presentation.html.
12. Nolan C. Counterfeit Components – Assessment Methodology and Metric Development Las vegas: IPC Apex Expo; 2014. Available from: http://thor.inemi.org/webdownload/2014/APEX/Counterfeit_Components_032614.pdf.

Downloaded on 2016-09-07 to IP 129.6.65.30 address. Redistribution subject to ECS terms of use (see ecsdl.org/site/terms_use) unless CC License in place (see abstract).

13. Semi.org. New SEMI Standards to Combat IC Chip Counterfeiting 2009 [November 11th, 2015]. Available from: http://www.semi.org/en/new-semi-standards-combat-ic-chip-counterfeiting-0.

14. Group O. Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.0, "Mitigating Maliciously Tainted and Counterfeit Products 2013 [November 11th, 2015]. Available from: https://www2.opengroup.org/ogsys/catalog/c139.

Downloaded on 2016-09-07 to IP 129.6.65.30 address. Redistribution subject to ECS terms of use (see ecsdl.org/site/terms_use) unless CC License in place (see abstract).

Josephson-Based Full Digital Bridge for High-Accuracy Impedance Comparisons

Frédéric Overney[1], Nathan E. Flowers-Jacobs[2], Blaise Jeanneret[1], Alain Rüfenacht[2], Anna E. Fox[2],
Jason M. Underwood[3], Andrew D. Koffman[3] and Samuel P. Benz[2]
[1]Federal Institute of Metrology METAS, Lindenweg 50, 3003 Bern-Wabern, Switzerland
[2]National Institute of Standards and Technology NIST, Boulder, CO 80305, USA
[3]National Institute of Standards and Technology NIST, Gaithersburg, MD 20899, USA
Email: frederic.overney@metas.ch

***Abstract*—This paper describes a Josephson-based impedance bridge capable of comparing any types of impedance over a large bandwidth. The heart of the bridge is a dual AC Josephson Voltage Standard (ACJVS) source which offers unprecedented flexibility in high-precision impedance calibration (i.e., calibration at arbitrary ratios and phase angles) allowing full coverage of the complex plane using a single bridge.**

***Index Terms*—Impedance comparison, ac coaxial bridge, AC Josephson voltage standard, digital bridge.**

I. Introduction

Impedance metrology makes intensive use of ac coaxial bridges for the realization of the capacitance, resistance and inductance scales at kilohertz frequencies. The type and complexity of the bridge depends on the type of the comparison: ratio bridge for the comparison of impedances of the same kind, quadrature bridge for comparing capacitance to resistance, and Maxwell-Wien or resonance bridge for comparing inductance to resistance and capacitance [1]. The common property of these measuring circuits is that once the bridge is balanced, the impedance ratio to be measured is directly given by a voltage ratio. The precise and accurate generation or measurement of this voltage ratio is therefore the cornerstone of all impedance metrology.

Prior to this work, the best voltage ratios were generated using transformers or inductive voltage dividers. However, the main drawback of such devices is that the voltage ratio is set at the fabrication stage of the transformer, by choosing the number of turns of the different windings, and the phase shift between the generated voltages is limited to either 0 or 180 degrees.

Programmable Josephson Voltage Standards (PJVS) can generate stable and precise stepwise approximated ac waveforms and were previously used to generate an accurate voltage ratio. The first two-terminal-pair bridge based on PJVS synthesized voltages was recently demonstrated [2]. This bridge was used to compare impedances of the same type ($R-R$ and $C-C$) with an accuracy comparable to transformer-based bridges over a frequency range from 20 Hz to 10 kHz. However, the large harmonic content of the PJVS waveform makes the comparison of impedances of different kinds ($R-C$, $R-L$ or $L-C$) more challenging [3] and limits the bandwidth to a few kilohertz.

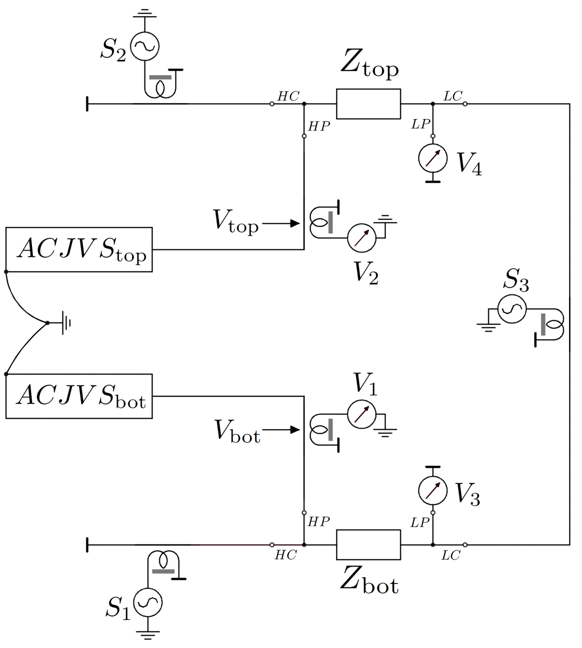


Fig. 1. Simplified bridge circuit of the JB-FDB. Once the bridge is balanced (i.e. $V_i = 0$, $i = 1...4$) by adjusting the amplitude and the phase of the bottom ACJVS source as well as the voltages S_i, $i = 1...3$, the complex impedance ratio is equal to the complex voltage ratio: $Z_{\text{bot}}/Z_{\text{top}} = -V_{\text{bot}}/V_{\text{top}}$.

On the other hand, ACJVS are perfect digital-to-analog converters that produce distortion-free waveforms with intrinsically accurate voltage over a bandwidth ranging from a few Hertz to 1 MHz. Combining and synchronizing two such ACJVS systems enables generation of a perfectly calculable voltage ratio with an arbitrary ratio and at any relative phase angle. In this work, these ideal voltage sources are implemented in a fully digital bridge able to compare any impedances with arbitrary ratios and phase shifts over a large bandwidth. In the near future, such bridges will greatly simplify the realization and maintenance of the various impedance scales in many NMIs around the world.

A brief description of the Josephson-Based Full Digital Bridge (JB-FDB) bridge as well as the preliminary results are given in the following sections.

U.S. Government work not protected by U.S. copyright

978-1-4673-9134-4/16/$31.00 ©2016 IEEE

II. Bridge Description

Figure 1 shows a simplified schematic of the JB-FDB developed for high accuracy comparison of two impedance standards $Z_{\rm top}$ and $Z_{\rm bot}$. The working principle of the JB-FDB is very similar to the digitally assisted bridge (DAB) recently developed at METAS [4] and can be summarized as follows: Once the bridge is balanced, i.e., once $V_i = 0$, $i = 1...4$, the four-terminal-pair definition of the two impedance standards is realized and the impedance ratio $Z_{\rm bot}/Z_{\rm top}$ is equal to the voltage ratio $-V_{\rm bot}/V_{\rm top}$. The main difference between the JB-FDB and the DAB is that the accurate and stable voltage ratio is generated using two ACJVS instead of a ratio transformer. In other words, the amplitudes and the phase of $V_{\rm bot}$ and $V_{\rm top}$ can each be set to any desired values, thus making the comparison of arbitrary impedances possible using a single bridge.

The two voltage sources required by the JB-FDB are provided by two independent pulse-driven ac Josephson voltage standards operated in separate Dewars of liquid helium. Each ACJVS system can generate a maximum rms voltage output of 1 V [5], [6] and each has an operating current range of 1.4 mA, that is, each can provide ± 0.7 mA of current compliance to a given input. The performance of the JB-FDB method relies on the intrinsic stability, linearity, and tunability of the two ACJVS systems. The relative phase stability of the two ACJVS pulse generators is guaranteed by having the two pulse generators share a 14.4 GHz clock and by triggering the start of both pulse generators using a fast rise-time trigger. The amplitude and phase of the two ACJVS output voltages are adjusted as part of the JB-FDB balancing procedure by recalculating the pulse pattern using a delta-sigma algorithm [7]. Each system can be controlled at the timing resolution of a single pulse, resulting in an approximate relative phase resolution of 70 ps.

III. First Results

The JB-FDB has been used to compare two impedances of 12.906 kΩ over a frequency range from 1 kHz to 20 kHz. The frequency dependence of the real part of the impedance ratio is shown in Fig. 2. For comparison, the same two impedance standards have been measured using the DAB and the result is also represented in Fig. 2.

The uncertainty bars represent the combined (k=1) uncertainties for the measurements made with the DAB while they correspond to the Type A uncertainties only for the measurements made using the JB-FDB. At a few frequencies, the comparison has been repeated a few times during several days, and corrections for the small but finite drift of the resistances have been applied. The residual spread of the results is larger than the Type A uncertainty and indicates that there remain some systematic effects that need to be further investigated.

Nevertheless, the good agreement between the results obtained with the JB-FDB and the DAB clearly shows, for the first time, the functionality of the ACJVS sources when implemented with an impedance bridge. Moreover, the potential accuracy of such a bridge is below 0.05 µΩ/Ω.

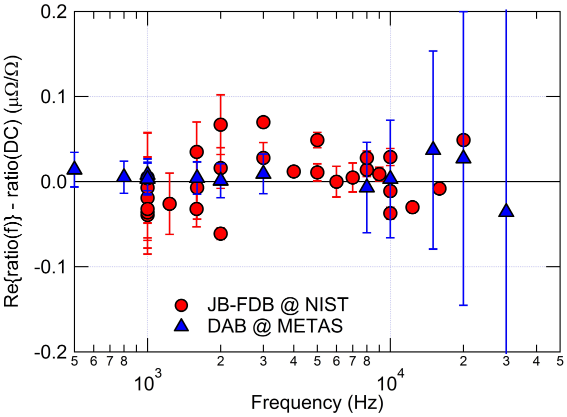


Fig. 2. Frequency dependence of real part of the ratio of two impedances of 12.906 kΩ measured at METAS with the DAB and at NIST with the JB-FDB.

IV. Conclusion

For the first time, two ACJVS systems have been integrated into a four-terminal-pair bridge, allowing the comparison of any impedances over a broad frequency range.

The first test of the bridge was carried out by comparing two resistances of 12.906 kΩ between 1 kHz and 20 kHz. The measured frequency dependence of the resistance ratios are in good agreement (<0.05 µΩ/Ω) with the frequency dependences measured with a classical analog bridge.

This digital bridge is an ideal tool for comparison of impedances of different kinds ($R-C$, $R-L$ or $L-C$) and for comparison of resistances having non-conventional ratios (10 kΩ to 12.906 kΩ, for example) as will be shown at CPEM in July.

Acknowledgment

The authors would like to thank B. Jeckelmann for his continuous support, P. Dresselhaus for the development and design of the ACJVS devices, and H. Bärtschi for his technical skills.

References

[1] S. Awan, B. Kibble, and J. Schurr. *Coaxial Electrical Circuits for Interference-Free Measurements*. IET electrical measurement series 13. Institution of Engineering and Technology, 2011.

[2] Jinni Lee, Jürgen Schurr, Jaani Nissilä, Luis Palafox, Ralf Behr, and Bryan P. Kibble. Programmable Josephson Arrays for Impedance Measurements. *IEEE Transactions on Instrumentation and Measurement*, 60(7):2596–2601, jul 2011.

[3] Luis Palafox, Ralf Behr, Jaani Nissila, Jurgen Schurr, and Bryan P Kibble. Josephson impedance bridges as universal impedance comparators. In *2012 Conference on Precision electromagnetic Measurements*, pages 464–465. IEEE, jul 2012.

[4] Frédéric Overney, Felix Lüönd, and Blaise Jeanneret. Broadband fully automated digitally assisted coaxial bridge for high accuracy impedance ratio measurements. *submitted to Metrologia*, 2016.

[5] Samuel P Benz, Steven B Waltman, Anna E Fox, Paul D Dresselhaus, Alain Rüfenacht, Logan A Howe, Robert E Schwall, and N. E. Flowers-Jacobs. Performance Improvements for the NIST 1 V Josephson Arbitrary Waveform Synthesizer. *IEEE Transactions on Applied Superconductivity*, 25(3):1–5, jun 2015.

[6] N. E. Flowers-Jacobs, A. E. Fox, P. D. Dresselhaus, R. E. Schwall, and S. P. Benz. Two-Volt Josephson Arbitrary Waveform Synthesizer. *submitted to IEEE Transactions on Applied Superconductivity*, 2016.

[7] J.C. Candy. *An Overview of Basic Concepts in Delta-Sigma Data Converters: Theory, Design, and Simulation*. IEEE Press, Piscataway, NJ, 1997.

"Josephson-Based Full Digital Bridge for High-Accuracy Impedance Comparisons."

2016 Spring Technical Meeting
Eastern States Section of the Combustion Institute
Hosted by Princeton University
March 13-16, 2016

Burning Velocities of Marginally Flammable Refrigerant-Air Mixtures[*]

John L. Pagliaro and Gregory T. Linteris

National Institute of Standards and Technology, Gaithersburg, Maryland

Refrigerant working fluids have been predicted to be large contributors to the increase in radiative forcing of the earth. Consequently, existing compounds will soon be phased out. Low-GWP replacements exist, but they tend to be mildly flammable, and there is a need to understand their flammability properties so that effective building codes and standards can be written to address their application. The burning velocities of interest are in the range of 1 cm/s to 10 cm/s, and hence are challenging to measure. To understand the challenges and properties of the new agents, experimental measurements and numerical predictions have been made for representative refrigerant-air mixtures. Burning velocities were measured using a constant pressure spherical chamber with high-speed imaging of the shadowgraph image of the propagating spherical flame. The flame propagation rate as a function of flame radius was used to estimate the effects of stretch, and to determine the un-stretched laminar burning velocity. For comparison, the burning velocity was also predicted numerically using a detailed kinetic mechanism for hydrofluorocarbon combustion developed at the National Institute of Standards and Technology (NIST).

1. Introduction/Background

Vapor-compression systems are widely used for refrigeration and for space conditioning in buildings. As a result of the Montreal Protocol [1], many of the high ozone-depletion potential (ODP) working fluids, for example the chlorofluorocarbons (CFCs), have been largely phased out. Their replacements, the hydrofluorocarbons (HFCs), have zero ODP, but like their predecessors, also have a large global warming potential (GWP). The contribution of the HFCs to the total radiative forcing of the Earth is projected to be large, estimated to be about 20 % of the total increase in radiative forcing between 2012 and 2050 [2]. Alternatives exist but have not been adopted largely because of the absence of building codes and standards for their safe use. Unfortunately, the properties that make these compounds break down in the troposphere, adding double bonds or hydrogen atoms, also makes them more flammable. Hence, flammability is an additional parameter that the Heating, Ventilation, Air-Conditioning, and Refrigeration (HVAC&R) industry must consider when optimizing the performance of working

[*] Official contribution of NIST, not subject to copyright in the United States. Certain commercial equipment, instruments, and materials are identified in this paper to adequately specify procedure. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology.

Pagliaro, John; Linteris, Gregory.
“Burning Velocities of marginally Flammable Regerant-Air Mixtures.”
Paper presented at the 2016 Eastern States Section Meeting of the Combustion Institute, Princeton, NJ, Mar 13-Mar 16, 2016.

fluids (beyond the presently considered thermodynamic, fluid dynamic, heat transfer and toxicological properties). The adopted working fluids will likely involve blends of individual compounds. To facilitate their safe use, it is essential for industry to have data on their combustion properties as well as a test metric to rank their flammability and predict their full-scale behavior.

As a first step in providing the required information, the present work examines two representative compounds: the pure agent R-32 (CH_2F_2) and its combination with R125 (C_2HF_5). Equal mass fractions of these two compounds comprise the refrigerant R410A, which is ubiquitous in residential air conditioners and heat pumps in the US, while the refrigerant R-32 is being used in Japan. The behavior of these two refrigerants is compared to that of the new low-GWP hydrofluoro-olefin (HFO) compound R-1234yf (CH_2CFCF_3), which has been of great interest recently as a substitute compound. The flammability of these compounds is discussed with regard to burning velocity, which is the subject of developing international codes and standards [3, 4], is a measure of the overall reactivity of the agent, and is used to simulate full-scale explosions [5, 6]. The present work experimentally measures and numerically predicts the un-stretched laminar burning velocity of CH_2F_2/C_2HF_5 mixtures with air, and determines the influence of stretch on burning velocity and ignitability.

2. Experiment and Data Reduction

The experimental and data reduction techniques used in this work are outlined below, with more details available in ref. [7]. The visually accessible 30 L spherical chamber and z-type shadowgraph system for high-speed video recording are based on the design of Faeth and coworkers [8-11] and Takizawa et al. [12]. Mixtures are prepared in the chamber via the partial pressure method, circulated for 3 minutes (using a metal bellows pump) to ensure complete mixing, then given 10 minutes to settle. The sample reactants are CH_4 (Matheson Tri-Gas, 99.97 % purity), C_3H_8 (Scott Specialty Gases, 99.0 % purity), C_2HF_5 (Allied Signal Chemicals, 99.5 % purity), CH_2F_2 (Honeywell, Genetron 32, 99.9 % purity), house de-ionized water, and house air that is filtered and dried. To initiate combustion, a capacitive discharge system generates a spark (with an estimated energy of 0.05 mJ to 500 mJ) at the center of the chamber. For each test, the ignition energy is gradually increased until ignition occurs, ensuring that the supplied energy is within an order of magnitude of the minimum ignition energy (MIE).

A high-speed camera and shadowgraph system provide images of the spherical flame propagation. Custom-developed image analysis software tracks the flame position (at the top, bottom, left, and right edges) as a function of time in the videos. For slow flames, buoyancy affects the burned gas velocity and the local stretch rate; the influence of buoyancy is minimized by using the flame propagation data only from the two horizontal directions [12-14]. The temporal evolution of the flame radius R_f yields the stretched flame speed, which is further processed to determine the burning velocity as a function of the stretch rate, as well as the un-stretched value (from extrapolation).

To capture the relationship between burning velocity and stretch rate, the range of flame radii included in the data reduction is limited, as recommended in the literature [14-19]. For example, the change in burning velocity with flame radius can be affected by such factors as confinement, radiation, ignition, and flame instabilities, depending on the size of the expanding sphere. Consequently, the upper bound R_{fU} is fixed at 3.5 cm for all tests to minimize confinement and radiation effects, and insure that all flame images were free of any cellularity. The lower bound of flame radii (R_{fL}) is also limited, to exclude data potentially influenced by the ignition event or extreme nonlinearity during the early stages of flame propagation. This latter effect (which is not always captured by current extrapolation methods) depends on the mixture Lewis number, and can lead to considerable errors in un-stretched results [16, 19]. Thus, the lower bound on included data R_{fL} ranges between 0.5 cm and 2.0 cm. The value is determined manually for each mixture by estimating (from a plot of R_f vs time) the value of R_f above which the curve is nearly linear. In a select number of cases, R_{fL} was set to 1.5 cm (ϕ = 0.90 and ϕ = 1.08) or 2.0 cm (ϕ = 0.96) so that the effects of extreme initial nonlinearity and ignition were both minimized.

For spherically symmetrical flame propagation, the flame speed in the laboratory reference frame corresponds to the burned gas velocity $S_b = dR_f /dt$, and is a function of the stretch rate, defined as $K = (2 / R_f)(dR_f / dt)$, where K is the stretch rate (s^{-1}), A_f is the flame surface area, and t is time [20]. As seen in the equation, the stretch rate decreases as the flame radius increases. Extrapolation to zero-stretch conditions is done using the relationship derived by Ronney and Sivashinsky [21] (for highly stretched flames with large Le), and later expressed in the following form by Kelley et al. [22],

$$S_b^0 t + c_1 = R_f + 2L_b \ln R_f - 4\frac{L_b^2}{R_f^2} - \frac{8}{3}\frac{L_b^3}{R_f^3}$$

in which the variable c_1 is an integration constant. The variables $S_b{}^0$, L_b, and c_1 are determined using a non-linear least squares optimization routine that fits the above equation to the experimentally measured flame radius versus time $R_f(t)$. From conservation of mass across the flame sheet, the un-stretched unburned gas velocity is then obtained from $S_u{}^0 = (\rho_b / \rho_u)\ S_b{}^0$, where $S_u{}^0$ is the unburned gas velocity, and ρ_u and ρ_b the unburned and burned gas densities. The burned gas is assumed to be in chemical equilibrium and ρ_b is calculated using the Sandia EQUIL routine [23]. Tests are performed at 296 ± 2 K and 101.33 kPa for each mixture. For each test, the extrapolation equations are fit to the R_f vs. t data from the left and right side flame tracking locations. The fitting parameters ($S_b{}^0$, L_b, and c) from the two sides are then averaged to produce the reported burning velocities and burned gas Markstein lengths.

The experimental system and data reduction methods were validated in previous work [7]. Fig. 1 (from ref. [7]) shows the un-stretched burning velocity $S_u{}^0$ using the present techniques for CH_4- and C_3H_8-air flames, over a range of fuel-air equivalence ratios, together with data from outwardly propagating flames (OPFs) [18, 24-26] and counterflow flames [27, 28]. Numerical predictions using the Wang mechanism [29] are shown by the dashed line. An (L) or (NL) next to the reference in the figure legend specifies whether the dataset was extrapolated using linear or non-linear methods. For both CH_4-air and C_3H_8-air flames, the burning velocities using the present methods are in excellent agreement with the previous results and with the numerical predictions.

The estimated uncertainties in the experimental determination of the burning velocity have been described in detail in ref. [7] for the same experimental apparatus (for hydrocarbon-air flames highly-inhibited by halogenated hydrocarbons). Uncertainties are reported as expanded uncertainties $U = ku_c$ determined from a combined standard uncertainty u_c and a coverage factor k = 2 corresponding to a level of confidence of 95 %. Based on those analyses, the maximum expanded relative uncertainty in S_u^0 is 13 %. However, measurement uncertainty is not the only cause of inaccuracy in the reported data. Buoyancy, radiation, and non-linear stretch effects can cause the inferred value of S_u^0 to differ from that of an ideal experiment, and this may vary with reactants. While these factors cannot be eliminated in the present study, their influence was minimized by using only the portion of the R_f vs. t data described above.

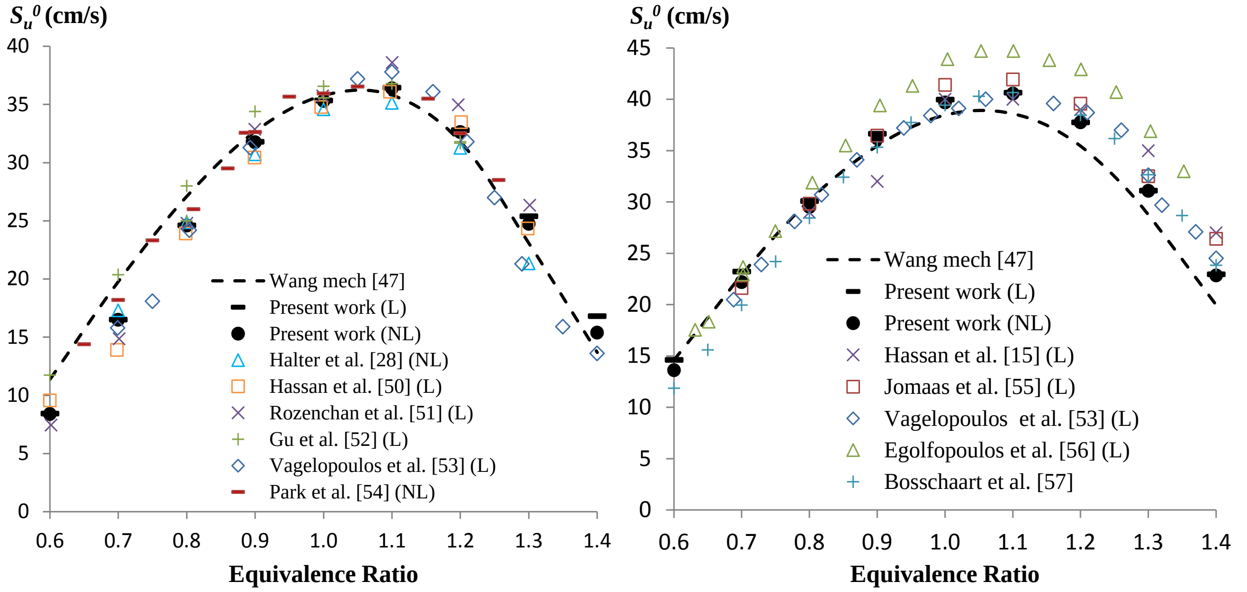


Fig. 1: Burning velocity of premixed CH_4-air (left) and C_3H_8-air (right) flames as a function of equivalence ratio, together with previously published results (symbols) and 1-D planar adiabatic simulation (dashed line). Figures (and references therein) from ref. [7].

3. Numerical Modeling

For the refrigerant-air flames, the flame structures and burning velocities are predicted with the Sandia PREMIX flame code and associated kinetics and transport processors [30-32], for reactants at an initial temperature and pressure of 298.15 K and 101.33 kPa. The Soret effect, and mixture-averaged molecular diffusion are included, and GRAD and CURV values are set to 0.05 to yield 310 to 420 active grid points. The comprehensive reaction mechanism (52 species and 621 reactions) is adopted from the NIST HFC mechanism [33, 34], with updates as described in refs. [7, 35]. The mechanism has been partially validated in earlier work, and more recently via burning velocity measurements and predictions for CH_4-air flames inhibited by C_2HF_5 [36].

"Burning Velocities of marginally Flammable Regeant-Air Mixtures."

4. Results and Discussion

Calculated Flame Temperatures and Burning Velocities for CH_2F_2 / C_2HF_5 Mixtures

The calculated adiabatic flame temperature T_{ad} (constant pressure, enthalpy) as a function of equivalence ratio for the CH_2F_2/C_2HF_5 mixtures in air is shown in Fig. 2. The equivalence ratio is based on the stoichiometeric reaction of the fuel mix to the most stable equilibrium products (typically HF, CO_2, COF_2, and H_2O, depending upon the fuel mix and ϕ). For CH_2F_2, the peak value ($T_{ad,max}$) is 2213 K, nearly the same as for methane-air flames (2230 K), while for pure C_2HF_5-air flames, $T_{ad,max}$ = 1805 K. Fig. 3 shows $T_{ad,max}$ and the value of ϕ at which the peak occurs, ϕ($T_{ad,max}$), as a function of the mass fraction of C_2HF_5 in the fuel $Y_{C_2HF_5}$. As illustrated, $T_{ad,max}$ decreases roughly linearly with increasing C_2HF_5 mass fraction, while ϕ($T_{ad,max}$), is constant at ϕ = 1.03. For the refrigerant R-410A mixtures ($Y_{C_2HF_5}$ = 0.5) in air, $T_{ad,max}$ = 1972 K.

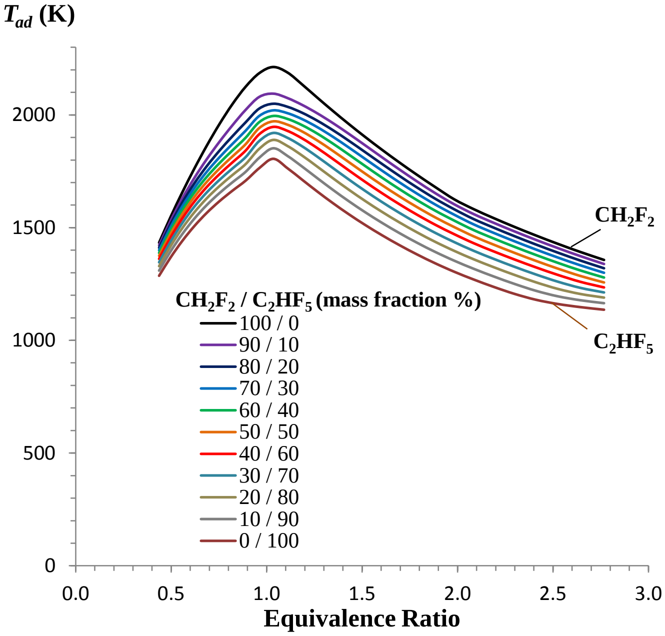


Fig. 2: Calculated adiabatic flame temperature for CH_2F_2/C_2HF_5 blends as a function of equivalence ratio.

The calculated un-stretched, planar, laminar, 1-D burning velocity S_u^0 as a function of the fuel-air equivalence ratio for CH_2F_2 / C_2HF_5 mixtures is shown in Fig. 4. As indicated, increasing the C_2HF_5 mass fraction from 0 % to 100 % decreases the peak burning velocity S_u^0,max from 5.95 cm/s to 0.56 cm/s, and changes the value of ϕ for S_u^0,max (ϕ(S_u^0,max)) towards leaner mixtures. As $Y_{C_2HF_5}$ increases above 60 %, however, the value of ϕ(S_u^0,max) abruptly shifts to a richer condition, ϕ = 1.2. This is illustrated more clearly in Fig. 5, which shows the peak burning velocity S_u^0,max and ϕ(S_u^0,max) as a function of the mass fraction of C_2HF_5 in the fuel. The peak burning velocity decreases smoothly until $Y_{C_2HF_5} \approx 0.70$, and then less rapidly as $Y_{C_2HF_5}$ increases further. While the ϕ($T_{ad,max}$) (from Fig. 3) is constant at 1.03 (for all mixtures), ϕ(S_u^0,max) (Fig. 5) is much lower for pure CH_2F_2–air mixtures at which ϕ(S_u^0,max) = 0.96, and becomes progressively leaner with added C_2HF_5, up to $Y_{C_2HF_5}$ = 0.6 at which ϕ(S_u^0,max) = 0.62. For a slight increase in $Y_{C_2HF_5}$ to 0.7, ϕ(S_u^0,max) increases abruptly to 1.2 and remains at the value for $Y_{C_2HF_5}$ = 0.8, 0.9, or

1.0. This behavior implies that at $Y_{C_2HF_5} \approx 0.65$, the kinetic pathways for reaction of the fuel mix changes significantly as compared to those that at lower C_2HF_5 loadings.

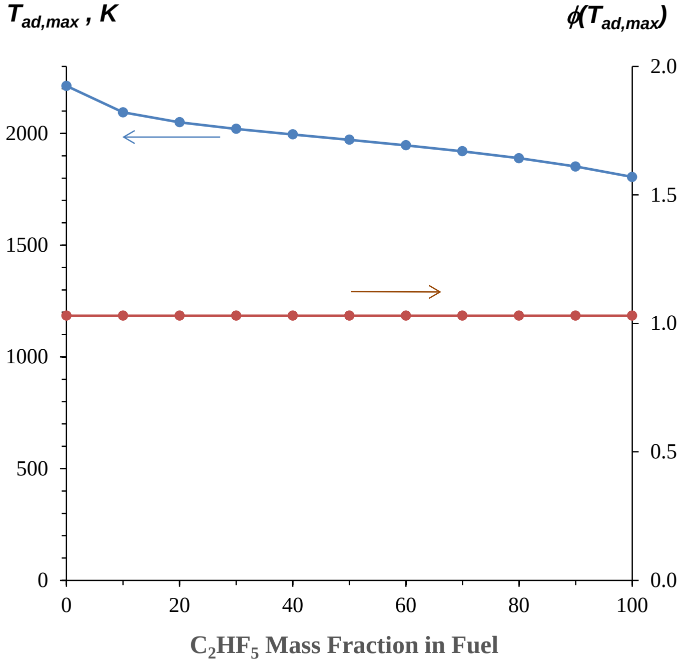


Fig. 3: Peak value of T_{ad} and the value of ϕ at the peak T_{ad} as a function of C_2HF_5 mass fraction in the fuel.

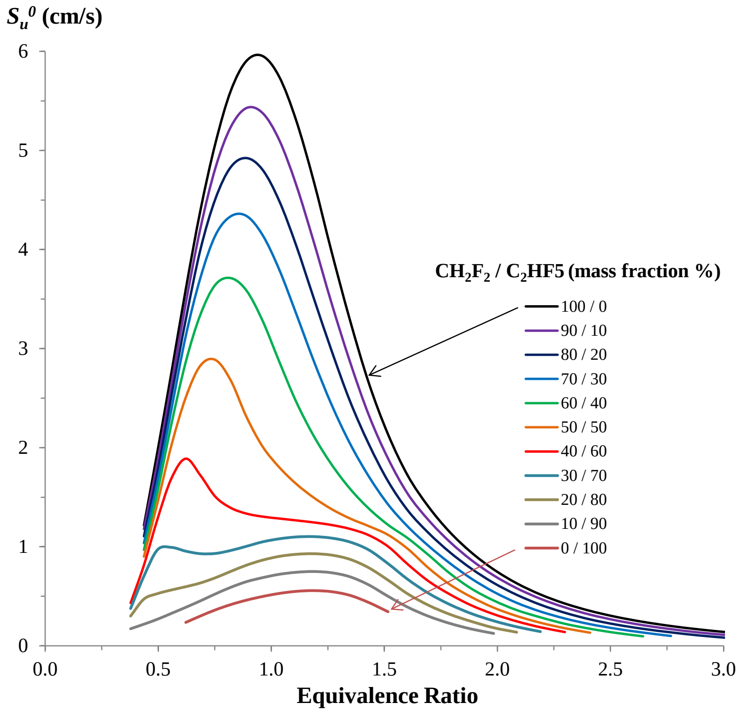


Fig. 4: Calculated burning velocity for CH_2F_2/C_2HF_5 blends as a function of equivalence ratio.

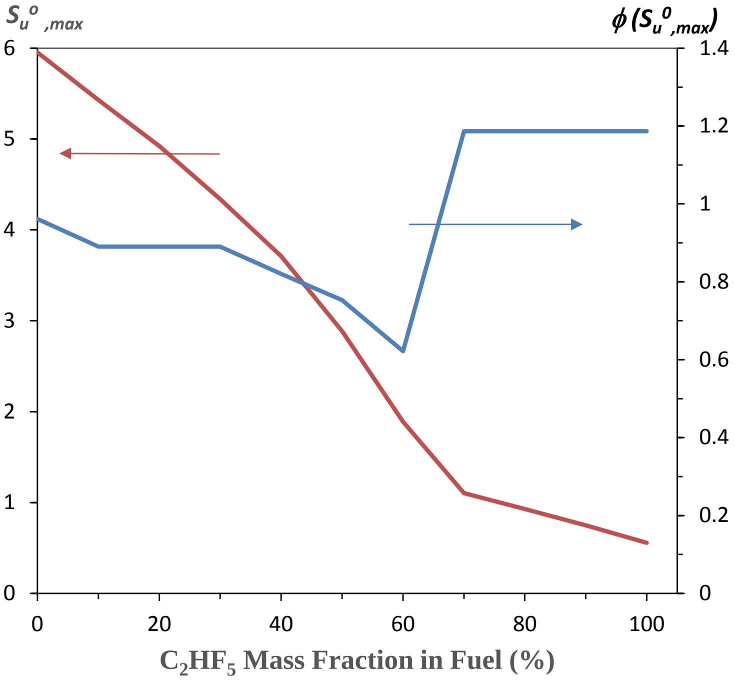


Fig. 5: Peak values of $S_u{}^0$ and the value of ϕ at the peak $S_u{}^0$, as a function of C_2HF_5 mass fraction in the fuel.

The magnitudes of the burning velocities in Fig. 4 are of interest in the context of flammability limits and explosion propensity. The 50/50 mix of CH_2F_2 / C_2HF_5 (R410A) has a calculated $S_u{}^0{}_{,\max}$ of 2.9 cm/s and is non-flammable as determined with ASTM-E-681. Nonetheless, the refrigerant R-1234yf (CH_2CFCF_3) in dry air has a measured $S_u{}^0{}_{,\max}$ = 1.2 cm/s and flammability limits of 6.8 % and 12 % [37]. That is, CH_2CFCF_3 has a peak burning velocity about 1/3 that of R410A, yet is flammable, while R410A is not. Since the Lewis number affects both flame stability [38-40] and critical radius for sustained propagation [41, 42], it is of interest to examine the response of these flames to stretch.

In order to gain confidence in the model predictions for the mixtures of CH_2F_2 and C_2HF_5, the calculated values of $S_u{}^0$ are first compared with experimental measurements in the following section.

Experimental Burning Velocities for CH_2F_2 –air and CH_2F_2 / C_2HF_5 –air Mixtures

The measured burning velocity of pure CH_2F_2 in dry air is shown in Fig. 6 together with other measurements from the literature [43-48] (which are not stretch corrected). For this refrigerant, the present measurements are somewhat higher than the others for $0.96 \leq \phi \leq 1.2$, and $S_u{}^0$ peaks at slightly leaner conditions ($S_u{}^0$ = 7.5 cm/s at $\phi \approx 0.96$) as compared to the other measurements ($S_u{}^0$ = to 6.1 cm/s to 6.7 cm/s, at $\phi \approx 1.03$ to 1.2). The numerical predictions (for a 1-D, steady, planar flame; dashed line in Fig. 6) yield a peak burning velocity of about 6 cm/s at ϕ = 0.95, which is somewhat lower, and at a leaner ϕ, than most of the measurements.

For the mixtures of air with 90 %/10 % CH_2F_2/C_2HF_5, the experimental measurements and numerically predicted burning velocities (Fig. 7) are in good agreement. Experiments were also attempted for leaner conditions for this mixture, as well as for other mixtures with increasing fractions of C_2HF_5; however, while ignition occurred for some conditions, sustained flame propagation could not be attained. For some conditions, the flames were initially ignited but then extinguished as the radius increased (a well-known effect in hydrocarbon-air flames due to the existence of a critical radius for sustained propagation). The unusually large critical radius for the lean flames, as well as the discrepancies in the experimental measurements in Fig. 6 may be due to Lewis number effects. Hence, the flame response to stretch for the present flames is examined.

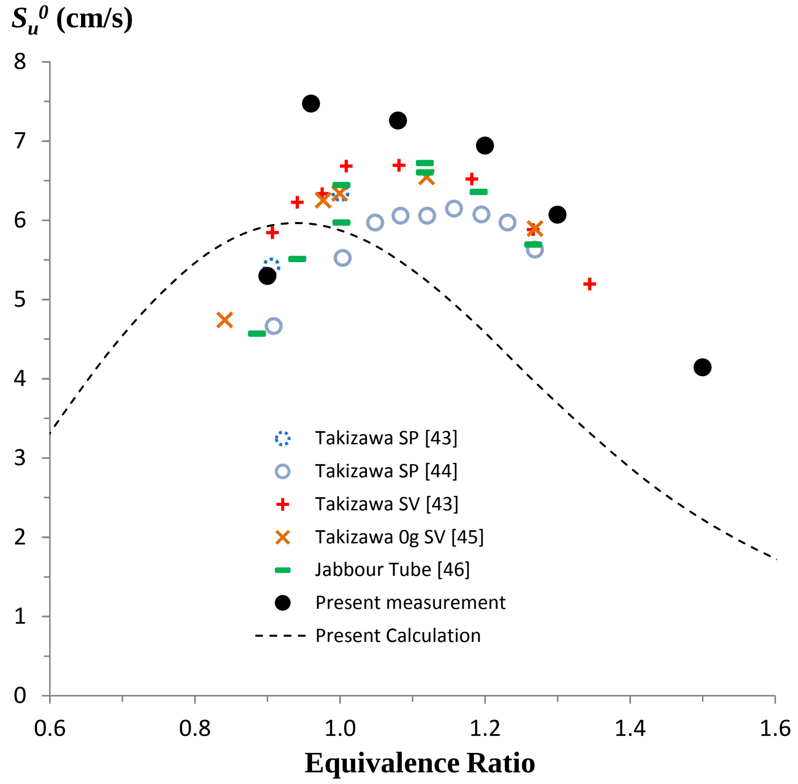


Fig. 6: Experimentally measured (points) and numerically predicted (lines) burning velocity of CH_2F_2-air flames (P_{init} = 101.33 kPa, T_{init} = 298 K) as a function of equivalence ratio (SP: schlieren photography, SV: spherical vessel).

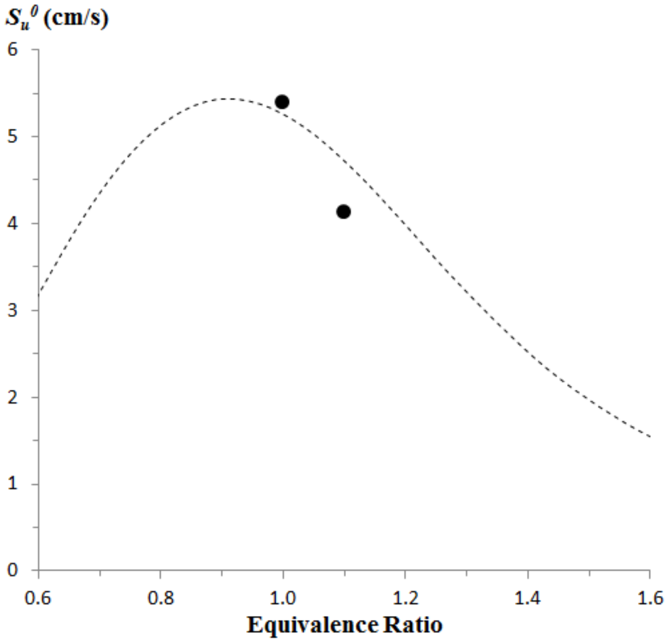


Fig. 7: Experimentally measured (points) and numerically predicted (lines) burning velocity of CH_2F_2 / C_2HF_5 – air flames (Y_{C2HF5} = 0.10, P_{init} = 101.33 kPa, T_{init} = 298 K) as a function of equivalence ratio.

Stretch Effects on Experimental Burning Velocities for CH_2F_2 –air Mixtures

As described above, in the present work, the un-stretched burning velocity S_u^0 is determined via a non-linear extrapolation of the stretched burning velocities obtained as a function of flame radius. The burned gas velocity S_b (dR_f /dt) vs. flame radius for the CH_2F_2-air flames is shown in Fig. 8. All flames show an increase in S_b with increasing flame radius; the effect is very mild for the richest flames (ϕ = 1.5), but increases as ϕ decreases, and is very strong for ϕ = 0.90, for which S_b approximately doubles as R_f increases from 1.4 cm to 3.5 cm. S_b is plotted as a function of stretch rate in Fig. 9. As illustrated, the un-stretched burned gas velocities S_b^0 (S_b at K = 0 s^{-1}) are higher than S_b at the largest radius, by up to 26 %. Moreover, the non-linear extrapolation may not be the best representation of the behavior at low stretch rates. For example, for the values of ϕ showing the most discrepancy between the present data and other data, different extrapolations to the zero stretch condition would produce better agreement with previous data. More research is needed to understand the proper treatment of the data for these fuels.

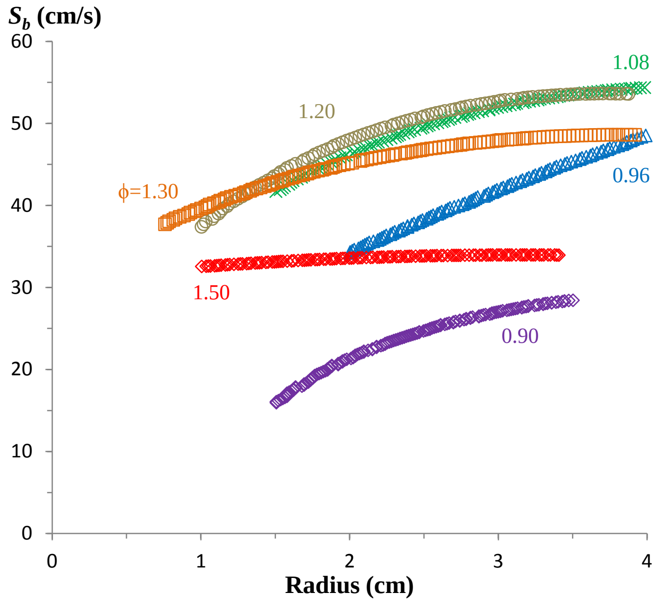


Fig. 8: Burned gas velocity S_b versus flame radius for CH_2F_2 in air at various equivalence ratios.

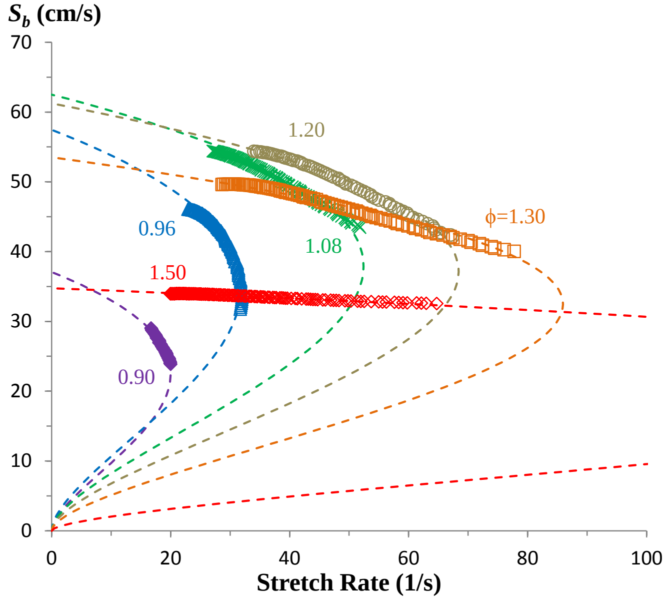


Fig. 9: Burned gas velocity S_b versus stretch rate for CH_2F_2 in air at various equivalence ratios (symbols are the experimental data and dashed lines are the non-linear fit).

Differences between the present data and previous measurements in different experiments may be due to the influence of stretch, or other factors. For example, the direct imaging experiments of outwardly propagating flames in refs. [43, 44] do not extrapolate to un-stretched conditions, and are subject to pressure rise in the chamber for flames at larger radii (chamber volume of 3.7 L). Other tests use a constant volume combustion bomb, either in normal gravity [43] or microgravity [45], and determine the burning velocity from measured pressure rise data. In each experimental run, data are obtained over a range of pressure and temperature of the unburned gases as the end gases are compressed by the advancing spherical flame. A curve is fit to the data of S_u vs. unburned gas temperature and pressure, and used to extrapolate back to reference conditions (P_{init} = 101.33 kPa, T_{init} = 298 K). As the radius increases, however, S_b is affected by both the changes in pressure and temperature, as well as differing stretch rates. Hence, it is not clear that the curve-fitting/extrapolation method is valid for these flames that are very sensitive to the stretch rate. Further, the hotter, higher pressure flames at larger radii may have greater radiative heat losses than typical hydrocarbon-air flames, since the product gases have an HF volume fraction of about 0.30, and HF is a strong radiator in the IR. The vertical tube experiment [46-48] , while it gives values similar to the other experiments (if the correct tube size is selected), is likely affected by flow in the unburned gases due to buoyancy and wall effects [44, 49]. The relative importance of these effects for the different experimental methods is unknown, and would be worthy of investigation in the future.

As shown in Fig. 6, the numerically predicted un-stretched burning velocities (steady, 1-D, planar) for CH_2F_2 – air disagree somewhat with the various experimental values (unsteady, 2-D or 3-D, spherical or cylindrical). This agreement is reasonable, however, considering the differences between the model and the experiments. The most important of these are likely the extrapolation to zero stretch rate, radiation heat losses, and the presence of buoyancy-induced flow, all of which are not included in the model. For example, near the edges of the horizontally propagating flames, buoyancy-induced flow in the burned and unburned gases may be modifying the stretch rate as compared to that estimated for a spherically propagating flame.

The Markstein lengths L_b of the present refrigerant-air flames can be determined from the curves in Fig. 9, and Fig. 10 and Fig. 11 show L_b as a function of ϕ for the pure CH_2F_2–air, and 90 % CH_2F_2/10 % C_2HF_5 – air flames, respectively. For the range of ϕ indicated on the figures, $L_b > 0$, and L_b increases at leaner conditions. These values of L_b are quite large: L_b for CH_2F_2 is about a factor of two larger than for propane at $\phi = 0.6$, and hydrogen-air flames at $\phi = 7$.

The Markstein lengths for CH_2CFCF_3-air mixtures has been estimated by Takizawa et al. [37]. For those mixtures, $L_b \approx -0.25$; i.e., is negative (i.e., the opposite of CH_2F_2-air flames) and is much smaller in magnitude, increasing slightly in magnitude for leaner flames. Moreover, L_b is also a function of the overall activation energy. As described by Takizawa at al. [37], the overall activation energy E_a of CH_2F_2-air flames is higher than that of CH_4-air flames, and E_a for CH_2CFCF_3-air flames is higher still. This is likely a result of a straight-chain reaction mechanism involving fluorine atoms (rather than the usual chain-branching radicals H, O, and OH), which has a high temperature dependence.

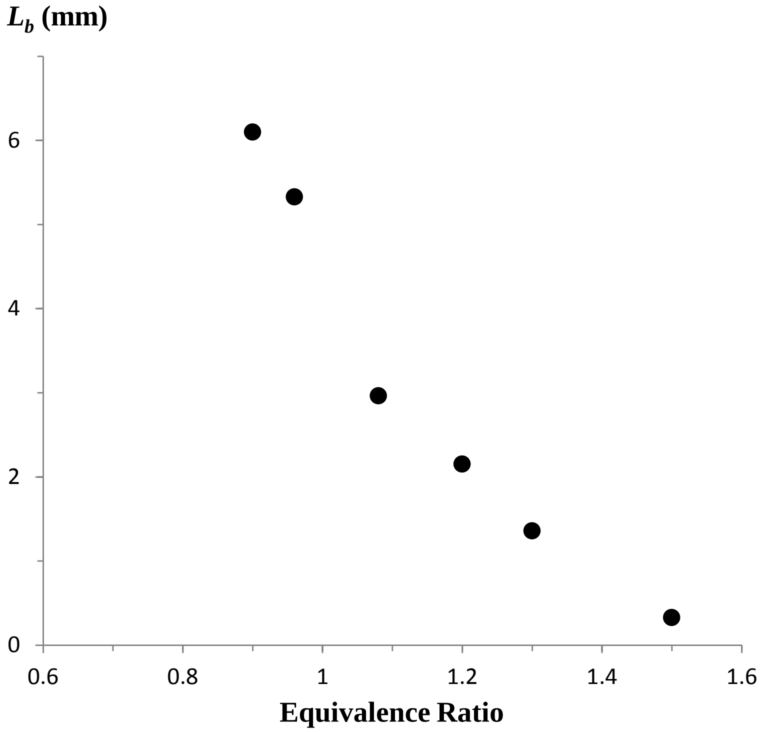


Fig. 10: Measured Markstein length for flames of CH_2F_2 in air at various equivalence ratios.

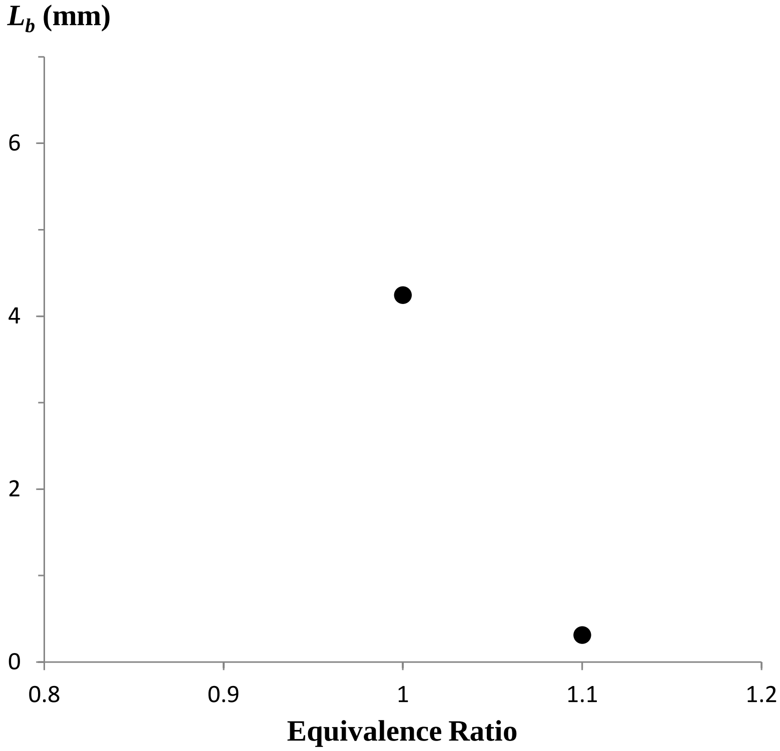


Fig. 11: Measured Markstein length for flames of 90 % CH_2F_2 / 10 % C_2HF_5 (mass fraction) in air at various equivalence ratios.

Lastly, the flame response to stretch, characterized by the Markstein length, can influence the turbulent burning velocity and thus influence the severity of ignition events at practical scales [50, 51]. Previous studies have shown that the turbulent burning velocity can depend on the mixture Lewis number, even for mixtures with the same laminar un-stretched burning velocity that are subject to the same turbulence intensity. This was shown for typical hydrocarbon- or hydrogen-air mixtures, and the CH_2F_2–air flames studied here have a much higher Markstein length and thus should have a larger response to flame stretch. Given the differing and high Markstein lengths of the refrigerant-air flames, consideration of the effects of stretch on the flame propagation may be important for understanding their full-scale flammability behavior.

5. Conclusions

The combustion behavior of two mildly flammable refrigerant-air mixtures has been studied. The burning velocity with respect to the product gases has been measured directly as a function of flame radius from shadowgraph images of the flame in an outwardly propagating flame configuration. Using a non-linear extrapolation to zero stretch, the un-stretched burning velocity with respect to the unburned gases S_u^0 has been estimated. For mixtures of CH_2F_2 in dry air, the burning velocity was measured for $0.90 \leq \phi \leq 1.5$. The present values of S_u^0 are within the range of previous measurements (not stretch-corrected) for $\phi = 0.9$ and $\phi = 1.5$, and 10 % to 20 % higher than previous measurements for near-stoichiometric flames ($0.96 \leq \phi \leq 1.3$). The present peak value of S_u^0 was 7.5 cm/s (at $\phi = 0.96$) as compared to the previous values (not stretch-corrected) of 6.1 cm/s to 6.7 cm/s (at $\phi = 1.03$ to $\phi = 1.6$). The extrapolated values of S_u^0 were 0 % to 26 % higher than the values of S_u at the largest radii with experimental data, illustrating that the nature of the extrapolation is likely to have a significant effect of the extrapolated values of S_u^0.

The value of S_u^0 was also calculated numerically using the Sandia PREMIX code together with a kinetic model for hydrofluorocarbon combustion. The predicted burning velocities peaked at a value of ϕ very close to the experiments, with $S_u^0 = 6.0$ cm/s, which was about 20 % lower than in the present experiment. The experiments showed a sharper reduction in S_u^0 for leaner conditions than did the simulations. For mixtures of CH_2F_2 and C_2HF_5 at mass fractions of 0.90 and 0.10, respectively, the peak burning velocity was about 5.4 cm/s, which agreed very well with the numerical prediction.

The influence of stretch on the burning velocity was estimated. The measured Markstein lengths of the CH_2F_2-air or CH_2F_2/CH_2CFCF_3-air flames were a strong function of the equivalence ratio, increasing for leaner flames, and were higher than typically found for hydrocarbon-air or hydrogen-air flames. Hence, the burning velocities of the refrigerant-air flames were very sensitive to the stretch, and lean flames had a very large critical radii. The present results imply that stretch effects are very important for understanding the flammability behavior and flame propagation of refrigerant-air mixtures, and their consideration is important for their safe use.

In future work, improved methods of extrapolation to zero stretch, as well as data at larger flame radii, would improve the accuracy of the values of S_u^0. Experiments at micro-gravity conditions would remove the effects of distortion due to buoyancy, which are possibly important in the present results, and will certainly be important for refrigerants with lower values of S_u^0. Data for a wider range of refrigerants (and their mixtures) would be helpful to refine the experimental and analytic methods. Improvements in the kinetic models, and their extension to new refrigerants, would be very helpful for analysis of the underlying chemical processes. Finally, inclusion of radiative heat losses in the burning velocity calculations, as well as direct numerical simulation of spherically propagating flames would be valuable, so that the experimental data could be used directly to validate the kinetic model (eliminating the need for extrapolation to zero-stretch conditions).

Acknowledgements

This work was supported by Boeing and a NIST-ARRA grant to JLP. The authors would like to thank Dr. Kenji Takizawa and Prof. Li Qiao for input concerning the experimental setup.

References

[1] The Montreal Protocol on Substances that Deplete the Ozone Layer as Adjusted and/or Amended in London 1990, Copenhagen 1992, Vienna 1995, Montreal 1997, Beijing 1999, UNEP.

[2] G. J. Velders, A. R. Ravishankara, M. K. Miller, M. J. Molina, J. Alcamo, J. S. Daniel, D. W. Fahey, S. A. Montzka, S. Reimann, Preserving Montreal Protocol climate benefits by limiting HFCs, Science 335 (2012) 922-923.

[3] ASHRAE, ANSI/ASHRAE Standard 34-2010, Designation and Safety Classification of Refrigerants, ASHRAE, Atlanta, GA USA, 2010.

[4] ISO, ISO/DIS 817, Refrigerants—Designation and safety classification. Currently in final draft International Standard stage, International Organization for Standardization, Geneva, Switzerland, 2010.

[5] O. R. Hansen, P. Hinze, D. Engel, S. Davis, Using computational fluid dynamics (CFD) for blast wave predictions, Journal of Loss Prevention in the Process Industries 23 (2010) 885-906.

[6] H. Hisken, G. Enstad, P. Middha, K. van Wingerden, Investigation of concentration effects on the flame acceleration in vented channels, Journal of Loss Prevention in the Process Industries 36 (2015) 447-459.

[7] J. L. Pagliaro, N. Bouvet, G. T. Linteris, Premixed flame inhibition by CF3Br and C3H2F3Br (2-BTP), Combust. Flame (submitted) (2015).

[8] L. K. Tseng, M. A. Ismail, G. M. Faeth, Laminar Burning Velocities and Markstein Numbers of Hydrocarbon/Air Flames, Combust. Flame 95 (1993) 410-426.

[9] S. Kwon, L. K. Tseng, G. M. Faeth, Laminar Burning Velocities and Transition to Unstable Flames in H2/O2/N2 and C3H8/O2/N2 Mixtures, Combust. Flame 90 (1992) 230-246.

[10] L. Qiao, C. Kim, G. Faeth, Suppression effects of diluents on laminar premixed hydrogen/oxygen/nitrogen flames, Combust. Flame 143 (2005) 79-96.

[11] M. I. Hassan, K. T. Aung, O. C. Kwon, G. M. Faeth, Properties of laminar premixed hydrocarbon/air flames at various pressures, Journal of Propulsion and Power 14 (1998) 479-488.

[12] K. Takizawa, A. Takahashi, K. Tokuhashi, S. Kondo, A. Sekiya, Burning velocity measurement of fluorinated compounds by the spherical-vessel method, Combust. Flame 141 (2005) 298-307.

[13] U. J. Pfahl, M. C. Ross, J. E. Shephard, Flammability Limits, Ignition Energy, and Flame Speeds in H2-CH4-NH3-N2O-O2-N2 Mixtures, Combust. Flame 123 (2000) 140-158.

[14] L. Qiao, Y. Gan, T. Nishiie, W. J. A. Dahm, E. S. Oran, Extinction of premixed methane/air flames in microgravity by diluents: Effects of radiation and Lewis number, Combust. Flame 157 (2010) 1446-1455.

[15] Z. Chen, M. P. Burke, Y. Ju, Effects of compression and stretch on the determination of laminar flame speeds using propagating spherical flames, Combust. Theory and Modelling 13 (2009) 343-364.

[16] Z. Chen, On the accuracy of laminar flame speeds measured from outwardly propagating spherical flames: Methane/air at normal temperature and pressure, Combust. Flame 162 (2015) 2442-2453.

[17] D. Bradley, P. H. Gaskell, X. J. Gu, Burning velocities, Markstein lengths, and flame quenching for spherical methane-air flames: a computational study Combust. Flame 104 (1996) 176-198.

[18] F. Halter, T. Tahtouh, C. Mounaïm-Rousselle, Nonlinear effects of stretch on the flame front propagation, Combust. Flame 157 (2010) 1825-1832.

[19] Z. Chen, M. P. Burke, Y. Ju, Effects of Lewis number and ignition energy on the determination of laminar flame speed using propagating spherical flames, Proc. Combust. Inst. 32 (2009) 1253-1260.

[20] F. A. Williams, A review of some theoretical considerations of turbulent flame structure, in: AGARD Conference Proceeding, AGARD-CP-164, NATO Science and Technology Organization, 1975,

[21] P. D. Ronney, G. I. Sivashinsky, A Theoretical Study of Propagation and Extinction of Nonsteady Spherical Flame Fronts, J. Appl. Math. 49 (1989) 1029-1046.

[22] A. P. Kelley, J. K. Bechtold, C. K. Law, Premixed flame propagation in a confining vessel with weak pressure rise, Journal of Fluid Mechanics 691 (2011) 26-51.

[23] A. E. Lutz, F. M. Rupley, R. J. Kee, W. C. Reynolds, E. Meeks, EQUIL: A CHEMKIN implementation of STANJAN for computing chemical equilibria, S. N. Laboratories, Reaction Design, Inc., 6500 Dublin Boulevard, Dublin, CA 94568. Software and manual authorized by Ellen Meeks and Fran Rupley, 1998.

[24] M. I. Hassan, K. T. Aung, G. M. Faeth, Measured and predicted properties of laminar premixed methane/air flames at various pressures, Combust. Flame 115 (1998) 539-550.

[25] G. Rozenchan, D. L. Zhu, C. K. Law, S. D. Tse, Outward propagation, burning velocities, and chemical effects of methane flames up to 60 atm, Proc. Combust. Inst. 20 (2002) 1461-1469.

[26] X. J. Gu, M. Z. Haq, M. Lawes, R. Woolley, Laminar Burning Velocity and Markstein Lengths of Methane-Air Mixtures, Combust. Flame 121 (2000) 41-58.

[27] C. M. Vagelopoulos, F. N. Egolfopoulos, Direct Experimental Determination of Laminar Flame Speeds, Proc. Combust. Inst. 27 (1998) 513-519.

[28] O. Park, P. S. Veloo, N. Liu, F. N. Egolfopoulos, Combustion characteristics of alternative gaseous fuels, Proc. Combust. Inst. 33 (2011) 887-894.

[29] G. Jomaas, X. L. Zheng, D. L. Zhu, C. K. Law, Experimental determination of counterflow ignition temperatures and laminar flame speeds of C2–C3 hydrocarbons at atmospheric and elevated pressures, Proc. Combust. Inst. 30 (2005) 193-200.

[30] R. J. Kee, J. F. Grcar, M. D. Smooke, J. A. Miller, A fortran computer program for modeling steady laminar one-dimensional premixed flames, Report No. SAND85-8240, Sandia National Laboratories, Livermore, CA, USA, 1991.

[31] R. J. Kee, G. Dixon-Lewis, J. Warnatz, R. E. Coltrin, J. A. Miller, A fortran computer package for the evaluation of gas-phase, multicomponent transport properties, Report No. SAND86-8246, Sandia National Laboratories, Livermore, CA, USA, 1986.

[32] R. J. Kee, F. M. Rupley, J. A. Miller, CHEMKIN-II: A fortran chemical kinetics package for the analysis of gas phase chemical kinetics, Report No. SAND89-8009B, Sandia National Laboratories, Livermore, CA, USA, 1989.

[33] D. R. Burgess, M. R. Zachariah, W. Tsang, P. R. Westmoreland, Thermochemical and chemical kinetic data for fluorinated hydrocarbons, Prog. Energy Combust. Sci. 21 (1995) 453-529.

[34] D. Burgess, M. R. Zachariah, W. Tsang, P. R. Westmoreland, Thermochemical and Chemical Kinetic Data for Fluorinated Hydrocarbons, Report No. NIST Technical Note 1412, Gaithersburg, MD, 1995.

[35] V. I. Babushok, G. T. Linteris, O. Meier, Combustion properties of halogenated fire suppressants, Combust Flame 159 (2012) 3569-3575.

[36] J. L. Pagliaro, G. T. Linteris, V. I. Babushok, Premixed flame inhibition C2HF3Cl2 and C2HF5, Combust. Flame 163 (2015) 54-65.

[37] K. Takizawa, K. Tokuhashi, S. Kondo, Flammability assessment of CH2=CFCF3: Comparison with fluoroalkenes and fluoroalkanes, Journal of Hazardous Materials 172 (2009) 1329-1338.

[38] C. K. Law, Dynamics of Stretched Flames, Twenty-Second Symposium on Combustion (1988) 1381-1402.

[39] P. Clavin, Dynamic Behavior of Premixed Flame Fronts in Laminar and Turbulent Flows, Prog. in Energy and Combust. Sci. 11 (1985) 1-59.

[40] M. Matalon, On flame stretch, Combust. Sci. Technol. 31 (1983) 169-181.

[41] A. P. Kelley, G. Jomaas, C. K. Law, Critical radius for sustained propagation of spark-ignited spherical flames, Combust. Flame 156 (2009) 1006-1013.

[42] Z. Chen, M. P. Burke, Y. Ju, On the critical flame radius and minimum ignition energy for spherical flame initiation, Proc. Combust. Inst. 33 (2011) 1219-1226.

[43] K. Takizawa, A. Takahashi, K. Tokuhashi, S. Kondo, A. Sekiya, Burning velocity measurement of fluorinated compounds by the spherical-vessel method, Combust. Flame 141 (2005) 298-307.

[44] K. Takizawa, N. Igarashi, K. Tokuhashi, S. Kondo, M. Mamiya, H. Nagai, Assessment of Burning Velocity Test Methods for Mildly Flammable Refrigerants, Part 2: Vertical-Tube Method, ASHRAE Trans. 119 (2013) 255-264.

[45] K. Takizawa, S. Takagi, K. Tokuhashi, S. Kondo, M. Mamiya, H. Nagai, Assessment of Burning Velocity Test Methods for Mildly Flammable Refrigerants, Part 1: Closed-Vessel Method, ASHRAE Trans. 119 (2013) 243-254.

[46] T. Jabbour, Flammable Refrigerant Classification Based on the Burning Velocity, Ph.D. Thesis, Ecole des Mines de Paris, Paris France, 2004.

[47] D. Clodic, T. Jabbour, Method of test for burning velocity measurement of flammable gases and results, HVAC&R Research 17 (2011) 51-75.

[48] T. Jabbour, D. F. Clodic, Burning Velocity and Refrigerant Flammability Classification, ASHRAE Trans. 110 (2004) 522-533.

[49] R. A. Strehlow, d. L. Reuss, Effect of a zero g environment on flammability limits as determined using a standard flammability tube apparatus, Report No. NASA-CR-3259, National Aeronautic and Space Administration, Washington, DC, 1980.

[50] J. B. Bell, R. K. Cheng, M. S. Day, I. G. Shepherd, Numerical simulation of Lewis number effects on lean premixed turbulent flames, Proc. Combust. Inst. 31 (2007) 1309-1317.

[51] F. Dinkelacker, B. Manickam, S. Muppala, Modelling and simulation of lean premixed turbulent methane/hydrogen/air flames with an effective Lewis number approach, Combust. Flame 158 (2011) 1742-1749.

ESTIMATION AND UNCERTAINTY QUANTIFICATION OF YIELD VIA STRAIN RECOVERY SIMULATIONS

Paul N. Patrone
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

ABSTRACT

In computational materials science, predicting the yield strain of crosslinked polymers remains a challenging task. A common approach is to identify yield via the first critical point of stress-strain curves produced by molecular dynamics simulations. However, the simulated data can be excessively noisy, making it difficult to extract meaningful results. In this work, we discuss an alternate method for identifying yield on the basis of residual strain computations. Notably, the associated raw data produce a sharper signal for yield through a transition in their global behavior. As we show, this transition can be analyzed in terms of simple functions (e.g. hyperbolas) that admit straightforward uncertainty quantification techniques.

1. INTRODUCTION

In computational materials science, estimating the yield strain ε_y of thermoset polymers remains a challenging task. Key difficulties arise from the general observations that: (I) these systems exhibit a continuous spectrum of relaxation times [1]; and (II) atomistic models are often necessary to capture the relevant physics of such relaxations [2]. As a result, it is becoming common for research groups to use molecular dynamics (MD) simulations in an effort to balance competing length and time-scale requirements [2].

While this approach offers a compromise that is often acceptable in R&D settings, it has nonetheless forced modelers to confront the inherent limitations of MD. In particular, high-throughput applications generally require the use of small (e.g. 5000 atom) systems, which exhibit large fluctuations in simulated data. In the case of yield, this means that standard estimation procedures (e.g. based on critical points of stress-strain curves) suffer from high levels of uncertainty that diminish the usefulness of the associated predictions (see, for example, Ref. [3]). This observation has led us to consider alternative methods of computing this quantity.

In this work, we propose to estimate yield strain through analysis of simulated residual-strain data. Analogous experimental results were obtained as far back as 1996 by Quinson *et al.*, who showed that residual strain of linear polymer chains (I) is zero up to yield, and (II) subsequently grows linearly with applied strain beyond yield [1]. Motivated by these results, we show how a global hyperbola analysis can be used to identify the onset of this linear behavior, and

Patrone, Paul.
"Estimation and uncertainty quantification of yield via strain recovery simulations."
Paper presented at the Composites and Advanced Materials Expo (CAMX) 2016, Anaheim, CA, Sep 27-Sep 29, 2016.

consequently yield. Moreover, we demonstrate how a bootstrap-style analysis of the resulting fit can be used to estimate uncertainties in the associated predictions, thereby quantifying our confidence in the simulations.

We emphasize that this analysis is limited to predicting yield and estimating uncertainties within the context of a single simulation. This is important insofar as finite-size and -time averaging can introduce an additional between-simulation uncertainty associated with under-sampling of crosslinked structures [4]. In the case of the glass-transition temperature, an analysis has been devised to quantify this additional "dark" uncertainty [4]. However, a comparable treatment for yield is complicated by the structure of the underlying stress and strain tensors. We leave further analysis for later work. Moreover, we do not rigorously pursue validation (or comparison with experiment), since open questions remain about verification (or estimation of uncertainties within the context of simulations alone).

2. OVERVIEW OF RESIDUAL STRAIN SIMULATIONS

In 1996, Quison et al. showed that deformation-relaxation experiments can be used to quantify the rate-dependence of relaxation modes in linear polymers such as polystyrene [1]. As a byproduct of this work, they generated plots of residual strain data ε_r as a function of the applied strain ε, where

$$\varepsilon_r = \frac{l_f(\varepsilon) - l_0}{l_0}$$

l_0 is the initial length in the loading direction, and l_f is the final length after applying a strain and then allowing the system to relax. Interestingly, they observed that yield (or the onset of plastic deformation) occurred at the first value of ε for which the material exhibited a non-zero residual strain. Although not discussed by the authors, it is also noteworthy that in all of their results, ε_r is approximately a linear function of the applied strain beyond yield. Critically, this observation holds irrespective of either the deformation rate, temperature, or relaxation time. Such results have since been experimentally reproduced for thermosets commonly found in aerospace applications [5].

Given the inherent length and time-scale limitations of MD, these observations are encouraging, since they suggest the possibility of a rate-independent method for determining yield *in silico*. We thus attempted to reproduce results in Ref. [5] using MD simulations of a roughly 5000 atom, 50/50 mixture of 4,4-diaminodiphenyl sulfone (44DDS) and digycidyl ether of Bisphenyl A (BisA), a two-functional epoxy. We refer to this system as 44BA. Details of the system preparation are provided in another manuscript [4,6], and we omit such a discussion here.

Figure 1 shows the results of a simulated residual-strain measurement, which is analogous to Fig. 4 in Ref. [5]. In order to generate this plot, we first strained the system by fixed, volume conserving increments at a variable rate determined by a convergence criterion on the running average stress; see Refs. [4,6] for details of how the convergence criterion works. After each strain increment, we saved the final structure for later analysis. Each simulation was a minimum of 20 ps long, with an average on the order of 60 ps to 80 ps. All strain simulations were performed using an NVT constraint with the Andersen thermostat at 300 K. Residual strains were then estimated (as a function of applied strain) by relaxing the saved unit cells with an NPT simulation and computing

$$\varepsilon_r = \sum_{i=1}^{3} \frac{\left|l_{f,i}(\varepsilon) - l_{0,i}\right|}{l_{0,i}}$$

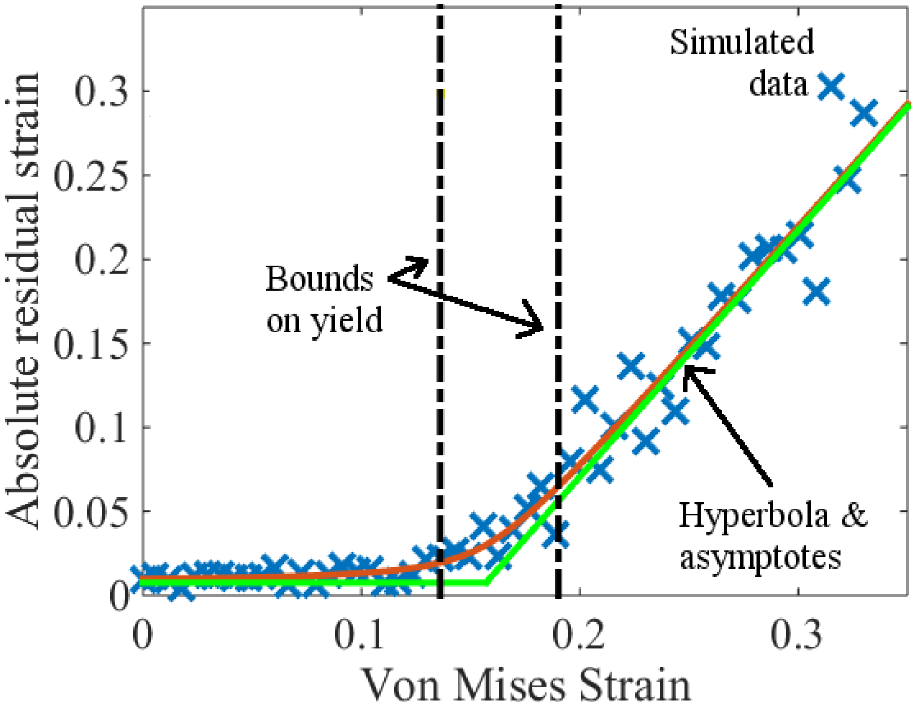


Figure 1: Simulated residual strain data showing a hyperbola fit and bounds on yield. The bounds are taken as the minimum and maximum values of yield computed via the synthetic dataset approach described below.

where $l_{f,i}$ and $l_{0,i}$ are the final and initial lengths of the ith side of the unit cell.[1] These latter simulations used the Parrinello barostat to ensure that the unit cells reached a well equilibrated, stress-free state. Analogous to before, a convergence criterion on the system dimensions was used to determine the simulation duration needed to reach an equilibrated state.

[1] We use a modified definition of residual strain (relative to Refs. [1] and [5]) because simulations provide additional information about deformation in three independent directions.

Several remarks are in order. Although noisy, the simulated residual strains show a bilinear character observed in experiments. In contrast to experiments, however, the simulated residual strains never fully go to zero for small applied strains. This occurs because the absolute values in our definition of ε_r transform thermal fluctuations into one-sided noise in ε_r. Moreover, the transition in ε_r associated with yielding is relatively smooth and occurs over a modest range of applied strains. Physically, we speculate that this arises from the fact that the anelastic relaxation mechanisms near yield have timescales that are poorly sampled by MD. In the next section, we show how hyperbola asymptotes can be used to estimate yield despite this lack of a sharp transition.

3. HYPERBOLA ANALYSIS AND UNCERTAINTY QUANTIFICATION

Given the data in Fig. 1, we estimate yield by first fitting a hyperbola *H* to our simulated applied and residual strains, ε_j and $\varepsilon_{r,j}$ (which are indexed by *j*). We find that it is convenient to use the parametrization

$$H = a + \frac{b}{2}\left(\varepsilon - \varepsilon_y\right) + \sqrt{\frac{b^2}{4}\left(\varepsilon - \varepsilon_y\right)^2 + e^c},$$

where a, b, c, and ε_y are free parameters that are determined by a least-squares procedure. We generically denote this collection of parameters as φ. Given these, we identify the yield strain ε_y with the hyperbola center, or equivalently the intersection of the hyperbola asymptotes. Physically we adopt the interpretation that these asymptotes characterize an "idealized" behavior of the simulation were it not to suffer from finite-size and -time effects.

In general, we find that a non-weighted least squares often gives reasonable estimates of yield, but not universally so. In particular, it is known that individual torsions in small-scale simulations can introduce large fluctuations into simulated quantities when a system is under high-strain [5]. Consequently, noise has a tendency to increase with the applied strain. In order to account for this, it is reasonable to determine ε_y via a weighted least-squares fit of the data to a hyperbola. Figure 1 shows a fit obtained from the following iterative procedure: (I) compute an unweighted estimate of the hyperbola *H*; (II) estimate a power law P(ε) for the residual data $H(\varphi, \varepsilon_j)$ - $\varepsilon_{r,j}$; (III) compute a weighted least-squares estimate of *H* with a weight-factor 1/P(ε). As the figure shows, this procedure allows for some flexibility in interpretation of the high-strain data while returning a reasonable estimate of yield.

To estimate uncertainties associated with our yield calculation, we perform a bootstrap-style analysis using repeated noise sampling of our model for the residual data. In particular, we define

$$\tilde{\varepsilon}_{r,j} = H(\varphi, \varepsilon_j) + \sqrt{P(\varepsilon_j)}N_j(0,1)$$

as a statistical model of residual strain data, where $P(\varepsilon_j)$ is determined according to the procedure described above, j indexes strain increments, and $N_j(0,1)$ are uncorrelated Gaussian random variables with mean zero and variance 1. Realizations of $\tilde{\varepsilon}_{r,j}$ are inexpensive to compute using random number generators. Hence, we use this noise model to generate thousands of synthetic datasets, which in principle have the same statistical structure as the original dataset. Applying the hyperbola analysis to these datasets then generates a distribution of yield values associated with our uncertainty in the fit procedure; see Fig. 2.

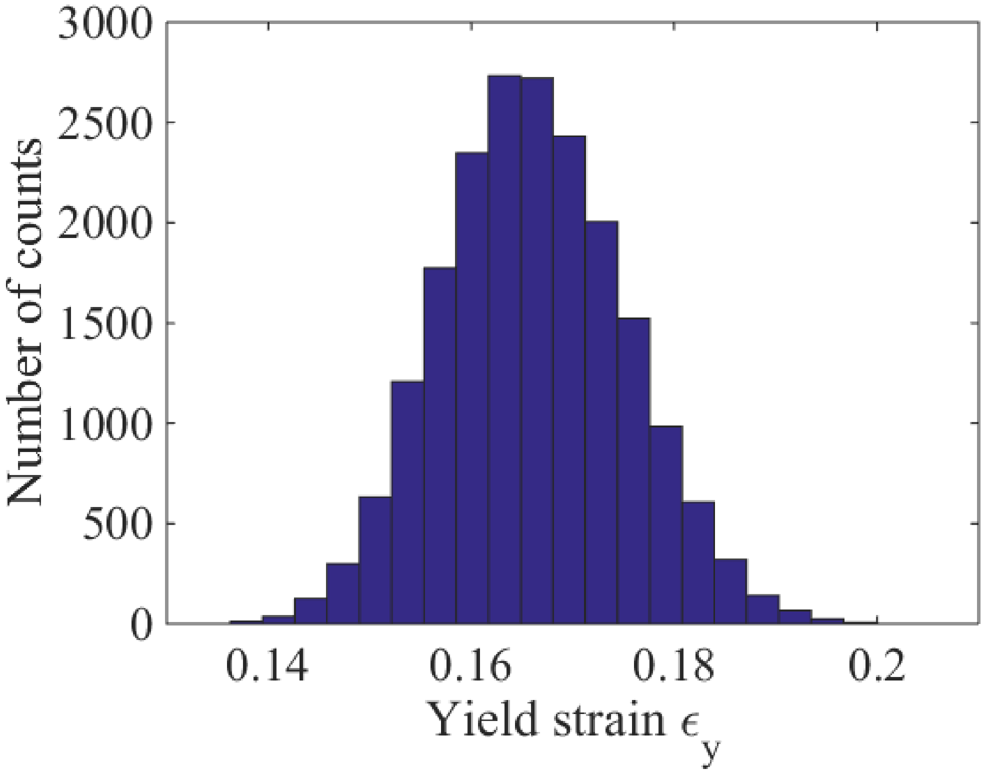


Figure 2: Histogram of yield values computed from repeated noise sampling of synthetic datasets.

4. CONCLUSIONS

Motivated by experimental work showing that the bilinear character of residual strain data is independent of strain rate, temperature, and relaxation times, we investigated how an analogous simulation protocol can be used to estimate yield. By analyzing the resulting data in terms of hyperbolas, we also showed how to (I) estimate the transition in residual strain that is associated with yield; and (II) quantify uncertainties in this procedure. We emphasize that in general, the methods discussed here only quantify uncertainties within the context of a single simulation. As previous work has shown, multiple simulations and comparison thereof may be necessary to construct a more complete picture of the computational predictions. However, qualitative agreement with experimental results warrants further investigation into the usefulness and validity of the method.

5. REFERENCES

1. Quinson, R., Perez, J., Rink, M. and Pavan, A. "Components of non-elastic deformation in amorphous glassy polymers." *Journal of Materials Science* **31** (1996): 4387-4394.

2. Li, C. and Strachan, A. "Molecular scale simulations on thermoset polymers: A review." *Journal of Polymer Science Part B: Polymer Physics* **53** (2) (2015): 103–122.

3. Sundararaghavan, V. and Kumar, A. "Molecular dynamics simulations of compressive yielding in cross-linked epoxies in the context of Argon theory." *International Journal of. Plasticity* **47** (2013): 111-125.

4. Patrone, P. N., Dienstfrey, A., Browning, A. R., Tucker, S., and Christensen, S., " Uncertainty quantification in molecular dynamics studies of the glass transition temperature." *Polymer* **87** (2016): 246-259.

5. Heinz, S., Tu, J., Jackson, M., and Wiggins, J. "Digital image correlation analysis of strain recovery in glassy polymer network isomers." *Polymer* **82** (2016): 87-92.

6. Patrone, P. N., Tucker, S., Dienstfrey, A. "Estimating yield-strain via deformation-recovery simulations." *In preparation.*

Annual Performance of a Two-Speed, Dedicated Dehumidification Heat Pump in the NIST Net-Zero Energy Residential Test Facility

W. Vance Payne, PhD
Member ASHRAE

ABSTRACT

A 2715 ft^2 (252 m^2), two story, residential home of the style typical of the Gaithersburg, Maryland area was constructed in 2012 to demonstrate technologies for net-zero energy (NZE) homes (or ZEH). The NIST Net-Zero Energy Residential Test Facility (NZERTF) functions as a laboratory to support the development and adoption of cost-effective NZE designs, technologies, construction methods, and building codes. The primary design goal was to meet the comfort and functional needs of the simulated occupants. The first annual test period began on July 1, 2013 and ended June 30, 2014. During the first year of operation, the home's annual energy consumption was 13039 kWh (4.8 kWh ft^{-2}, 51.7 kWh m^{-2}), and the 10.2 kW solar photovoltaic system generated an excess of 484 kWh. During this period the heating and air conditioning of the home was performed by a novel air-source heat pump that utilized a reheat heat exchanger to allow hot compressor discharge gas to reheat the supply air during a dedicated dehumidification mode. During dedicated dehumidification, room temperature air was supplied to the living space until the relative humidity setpoint of 50% was satisfied. The heat pump consumed a total of 6225 kWh (2.3 kWh ft$^{-2,}$ 24.7 kWh m^{-2}) of electrical energy for cooling, heating, and dehumidification. Annual cooling efficiency was 10.1 Btu W^{-1}h^{-1} (2.95 W W^{-1}), relative to the rated SEER of the heat pump of 15.8 Btu W^{-1}h^{-1} (4.63 W W^{-1}). Annual heating efficiency was 7.10 Btu W^{-1}h^{-1} (2.09 W W^{-1}), compared with the unit's rated HSPF of 9.05 Btu W^{-1}h^{-1} (2.65 W W^{-1}). These field measured efficiency numbers include dedicated dehumidification operation and standby energy use for the year. Annual sensible heat ratio was approximately 70%. Standby energy consumption was 5.2 % and 3.5 % of the total electrical energy used for cooling and heating, respectively.

INTRODUCTION

Buildings consumed 41% of all energy used in the United States in 2010, with residential buildings and commercial buildings accounting for 22% and 19%, respectively. In addition to consuming more energy than the transportation or industrial sectors, buildings represent the fastest growing sector of energy usage (DOE 2010). In order to support reductions building energy consumption, many buildings have been designed, constructed and monitored throughout the world to demonstrate the feasibility of achieving net-zero energy.

Parker (2009) presents a history of low energy homes and presents annual performance data from a dozen very low energy homes in North America. In Washington D.C. in 2001, a 2885 ft^2 (268 m^2) modular ZEH called the "Solar Patriot" or Hathaway home was built to demonstrate a ZEH in a mixed humid climate. An advanced geothermal heat pump was used for space conditioning. A 6 kW photovoltaic (PV) system was installed with the

W. Vance Payne is a Mechanical Engineer with the HVAC&R Equipment Performance Group, Energy and Environment Division, National Institute of Standards and Technology, U.S. Dept. of Commerce, Gaithersburg, MD 20899: vance.payne@nist.gov.

Payne, William.
"Annual Performance of a Two-Speed, Dedicated Dehumidification Heat Pump in the NIST Net-Zero Energy Residential Test Facility."
Paper presented at the ASHRAE Winter Conference 2016, Orlando, FL, Jan 23-Jan 27, 2016.

objective of reaching zero energy on an annual basis. The Hathaway home is in the same weather region as the NIST home and offers some electric energy use comparisons.

Musall et al. (2010) summarizes the research of the International Energy Agency's Annex 52 "Towards Net Zero Energy Buildings" and states that "during the last 20 years more than 200 reputable projects with the claim of a netzero energy budget have been realized all over the world."

Sherwin et al. (2010) present the performance of four near net-zero energy homes in Florida instrumented to provide data on electrical consumption and generation, indoor conditions, and outdoor weather. NZEH#2 used a 19 SEER air conditioner (AC) for cooling and averaged 216 kWh month^{-1} for cooling alone while maintaining an average dry-bulb temperature of 78.3°F (25.7°C) and 52.2% RH; standby power was 55 W. NZEH#3 used a ground-source heat pump (GSHP) and averaged 453 kWh in September of 2008 for cooling in a northern Florida climate. NZEH#4 used a 18.4 SEER two-speed air source heat pump with 9.1 HSPF using 3444 kWh, 24% of the total electric use, for cooling and heating while operating at low speed 85% of the time with indoor conditions averaging 75.7°F (23.7 °C) and 54.5% RH. Appliance loads were not separately measured for any of these NZEH sites.

TEST HOUSE

The net-zero energy residential test facility, NZERTF, is a unique facility that resembles a residence yet is truly a laboratory (Figure 1). The house is two stories having 2715 ft^2 (252 m^2) of living area, a 1453 ft^2 (135 m^2) fully conditioned basement, and an 1162 ft^2 (108 m^2) conditioned but unoccupied attic (Petit et. al 2015). The water, lights, and appliance usage utilized by a family of four were simulated in the NZERTF according to occupancy schedules, which can be found in Omar and Bushby (2013) and Kneifel (2012). Sensible heat energy generated by occupants was simulated in various rooms, but internal latent load simulation was concentrated in the kitchen. Though natural gas could be supplied to the house, during the first year of operation all of the equipment and appliances were powered by electricity either from the site's 10.2 kW (DC) solar photovoltaic (PV) system or the main power grid. The building envelope was constructed using a continuous air barrier system to minimize infiltration, and ventilation was provided by a heat recovery ventilator, HRV. A whole house pressurization or blower door test conducted after the house was complete yielded a leakage rate of 472 cfm (802 m^3/h) at 0.20 in H_2O (50 Pa) corresponding to 0.63 air changes per hour. HVAC operations consumed 51% of all electrical energy used on the site.

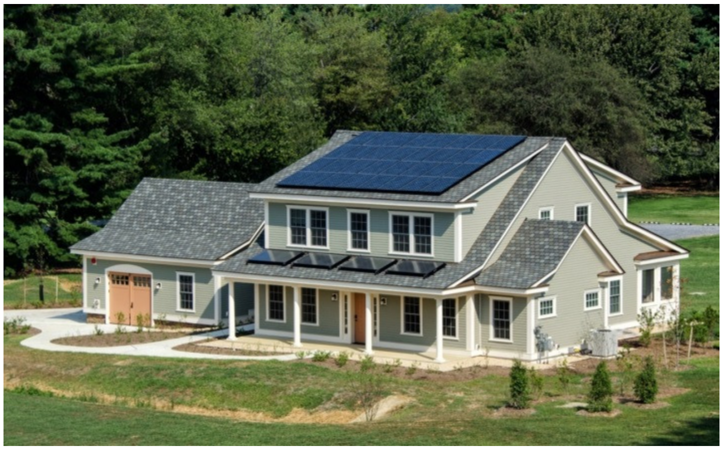


Figure 1 Net-zero energy residential test facility.

AIR-TO-AIR HEAT PUMP SYSTEM

The heating and air conditioning system used for the first year of operation in the NZERTF consisted of a HP system that incorporates a dedicated dehumidification cycle (Figure 2). The air distribution duct system was designed for less than 0.5 in H_2O (124.5 Pa) external static pressure drop at the air handler with supply and return duct airflow rates of 1200 cfm (2039 m^3 h^{-1}) with all registers fully open. The outdoor unit incorporates a two-speed scroll compressor with two modulated hot gas valves on the compressor discharge that send hot refrigerant gas through a third pipe to the indoor reheat heat exchanger during active dehumidification. A supply air temperature sensor provides the control signal used to proportionally modulate the flow of hot refrigerant gas to maintain a preset supply temperature during dedicated dehumidification. The indoor air handler unit contains a variable-speed indoor fan. At the Air-Conditioning, Heating, and Refrigeration Institute (AHRI) rating condition (AHRI 2008), the A-Test cooling capacity is 26 kBtu h^{-1} (7.60 kW) and the EER (COP) is 13.05 Btu W^{-1} h^{-1} (3.82 W W^{-1}). In the heating mode at AHRI rating condition, the unit has a heating capacity of 26.6 kBtu h^{-1} (7.80 kW). The unit has a seasonal energy efficiency ratio (SEER) of 15.8 Btu W^{-1} h^{-1} (4.63 W W^{-1}) and a heating seasonal performance factor (HSPF Region IV) of 9.05 Btu W^{-1} h^{-1} (2.65 W W^{-1}).

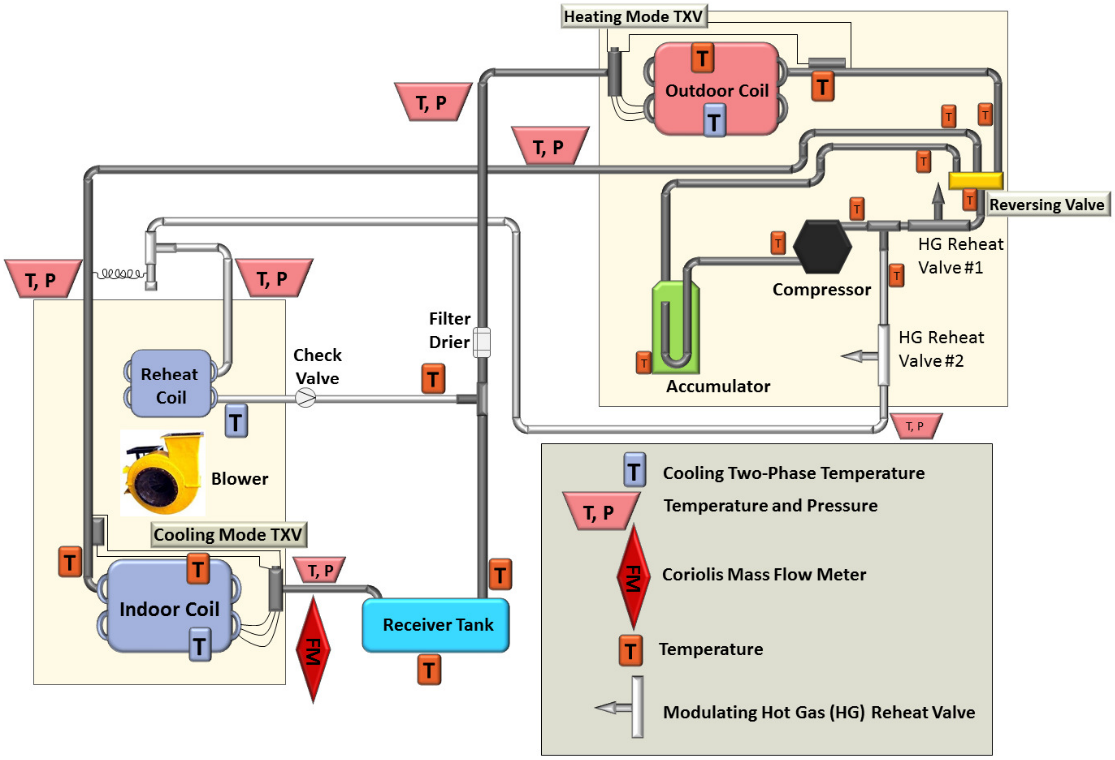


Figure 2 Heat pump refrigerant circuiting and instrumentation.

INSTRUMENTATION AND UNCERTAINTY

The heat pump system was instrumented to monitor operational parameters and efficiency. The refrigerant circuit is shown in Figure 2 with temperature, pressure, and refrigerant mass flow sensors identified. The HP has its own dedicated data acquisition system that continuously monitors both refrigerant and air side conditions. Air side capacity (sensible and latent) and component power demand are continuously measured to give instantaneous values of efficiency (COP). The heat pump instrumentation, data acquisition system, and measurement uncertainty, as well as all other electrical/mechanical subsystems within the NZERTF are described in Davis et al. (2014).

COOLING AND HEATING SEASON PERFORMANCE

The heat pump was operated as a single zone system with a thermostat located in the living room area on the first floor. During heating mode or defrost mode operations, the indoor unit controller could energize up to 10 kW of electric resistance heat. The thermostat setpoints in the cooling and heating modes were 75.0°F (23.8°C) and 70.0°F (21.1°C), respectively, without setback.

Table 1: Instrumentation Uncertainty for the Air-Source Heat Pump

Instrument	Range	Total Uncertainty at the 95 % Confidence Level
Transducer voltage measurement	0 to 10 VDC	±5 mVDC
T-type thermocouples	16°F to 131°F (-10°C to 55°C)	±1.0°F (0.6°C)
Barometric pressure	20 to 30 in Hg (0.667 to 1.001 bar)	±1 % of reading
High pressure transducer	1000 psig (6895 kPa)	±0.25 % of reading
Low pressure transducer	500 psig (3447 kPa)	±0.25 % of reading
Air pressure differential (ESP[1])	0 to 0.75 in H_2O (0 to 187 Pa)	±0.8 % of reading
Indoor blower and controls power meter	0 to 300 VAC, 5 Amps, 1000 W	±5 W
Indoor total power meter	0 to 300 VAC, 100 Amps, 20 000 W	±100 W
Outdoor unit power meter	0 to 300 VAC, 20 Amps,4000 W	±20 W
Supply air dry-bulb temperature sensor	-20°F to 120°F (-28.8°C to 49°C)	±0.9°F (0.5°C)
Supply air dew-point temperature sensor	-20°F to 120°F (-28.8°C to 49°C)	±1.8°F (1.0°C)
Return air dry-bulb temperature sensor	-40°F to 140°F (-40°C to 60°C)	±0.4°F (0.2°C)
Return air dew-point temperature sensor	-4°F to 212°F (-20°C to 100°C)	±1.5 % of reading
Outdoor air dry-bulb temperature sensor	-40°F to 140°F (-40°C to 60°C)	±0.4°F (0.2°C)
Outdoor air dew-point temperature sensor	-4°F to 212°F (-20°C to 100°C)	±1.5 % of reading
Coriolis refrigerant mass flow meter	0 to 80 lbm min^{-1} (0 to 2180 kg h^{-1})	±0.15 % of reading

1-External Static Pressure

Measured cooling and heating thermal energy for the heat pump can be seen in Table 2. For the entire cooling season the heat pump produced a seasonal COP of 10.07 Btu W^{-1} h^{-1} (2.95 W W^{-1}) (Figure 3a). Although not directly comparable, this seasonal COP was 36% lower than the rated SEER of the system. The measured performance was lower than the rated SEER value due in part to different indoor setpoint conditions than the standardized tests, as well as differences in the cumulative outdoor temperature conditions, ventilation thermal loads, and standby power demand. Heating thermal loads are also shown in Table 2 with their associated monthly COP in Figure 3b. For the entire heating season COP of the system was 6.96 Btu W^{-1} h^{-1} (2.04 W W^{-1}), a value that was 23% lower than the rated HSPF. The resistance heat operated more frequently than anticipated in the heating season due to the inherent control logic of the thermostat. The thermostat heating configuration allows the installer or homeowner to prescribe differential temperatures relative to the current setpoint temperature and to prescribe delay times (the maximum amount of time a given stage is allowed to operate) before energizing the next higher stage. The delay time control logic appears to be effective in the cooling mode, but produced unnecessary usage of electric resistance heat in the heating mode. By limiting the 2nd stage delay time to a maximum of 40 min, the thermostat required 3rd stage electric heat even though 2nd stage heating was increasing the temperature in the house.

DEDICATED DEHUMIDIFICATION PERFORMANCE

In the cooling mode, the thermostat was set such that the dedicated dehumidification mode of the HP unit was engaged if the relative humidity (RH) reached 50%. Studies of high performance homes with mechanical ventilation showed that the HVAC systems were generally able to maintain the conditioned space below 60% RH (Rudd et al. 2014). An RH setpoint of 50% was selected for the NZERTF to be more restrictive and more comfortable.

Table 2: Cooling and Heating Thermal Loads

Cooling, kWh						
Jul-2013	Aug-2013	Sep-2013	Oct-2013	Apr-2014	May-2014	Jun-2014
2123	1621	937	306	67	603	1560

Heating, kWh						
Oct-2013	Nov-2013	Dec-2013	Jan-2014	Feb-2014	Mar-2014	Apr-2014
56	832	1351	2157	1635	1423	253

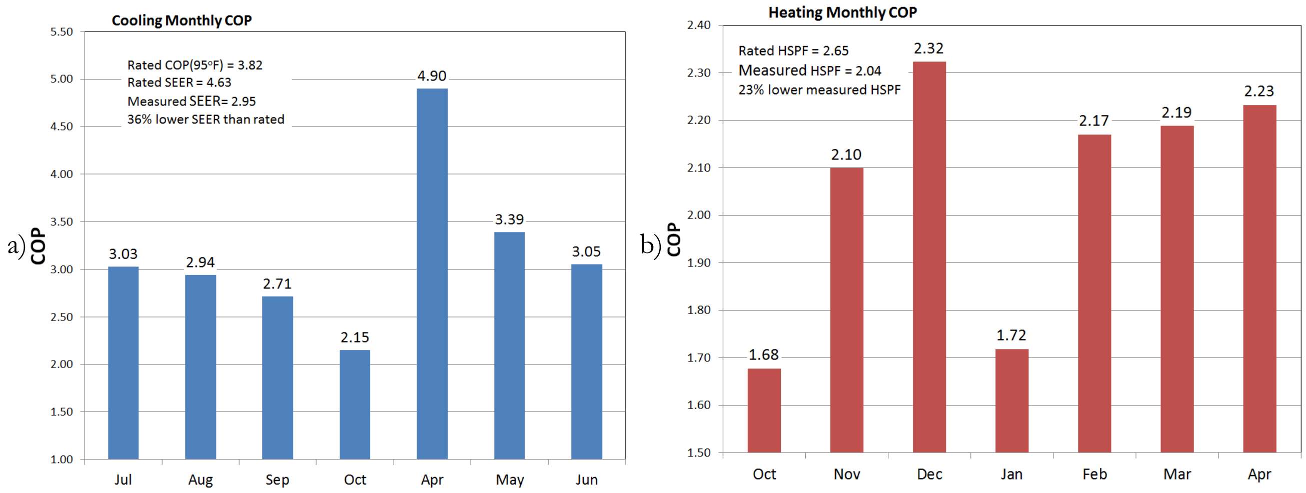


Figure 3 Cooling (a) and heating (b) season COP.

Dedicated dehumidification control consists of two distinct stages: stage 1 lowers the indoor blower speed for approximately 15 min or until the RH setpoint is reached; stage 2 begins after 15 min of stage 1 operation by modulation of the two outdoor unit hot gas bypass valves to control indoor supply air temperatures to a pre-selected "room neutral" temperature. Table 3 shows the operating times and electrical energy use during active dehumidification. Active dehumidification consumed approximately 892 kWh of electrical energy, or 6.8 % of all the house electrical energy used during the first year of operation. Figure 4a shows the operational dehumidification efficiency (or energy factor) in units of liters per kilowatt hour. The U.S. Environmental Protection Agency issues Energy Star ratings for dehumidifiers (< 75 pints day^{-1} or 35.5 liter day^{-1}) with efficiencies of 1.85 L kWh^{-1} or greater (EPA 2015). While the HP dedicated dehumidification efficiency was lower than Energy Star, this mode of dehumidification does not add heat to the conditioned space as do most portable dehumidifiers.

Table 3: Active Dehumidification Mode Runtimes

Active Dehumidification with Reheat Runtime (min)						
Jul-2013	Aug-2013	Sep-2013	Oct-2013	Apr-2014	May-2014	Jun-2014
9891	9510	4198	2280	0	829	7989
Active Dehumidification Electrical Energy (kWh)						
246	246	114	60	0	22	204

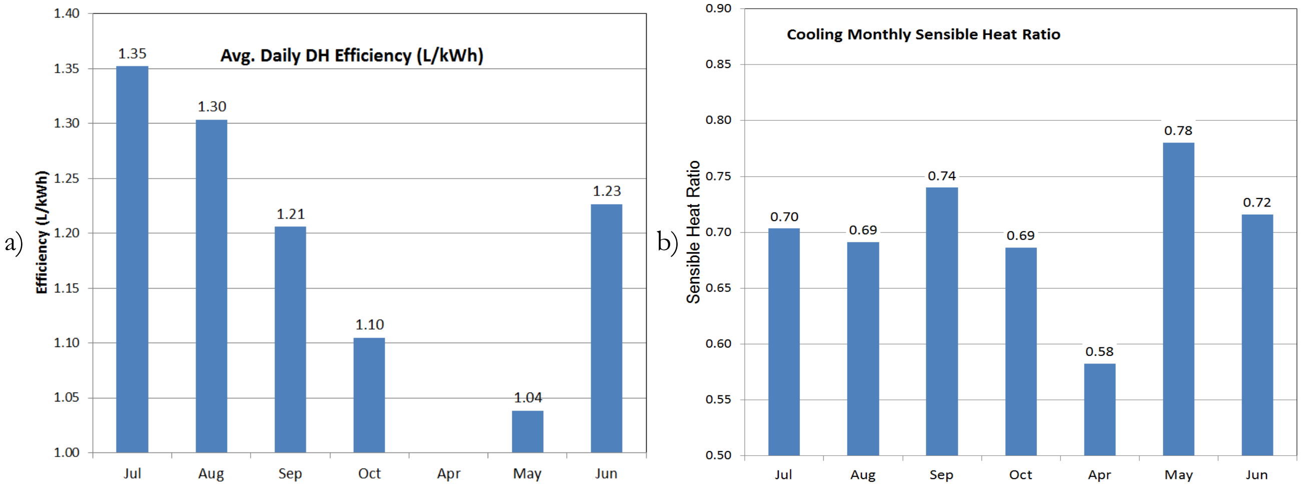


Figure 4 Dedicated dehumidification mode efficiency (a) and sensible heat ratio while maintaining 50% RH (b).

A key feature of the NIST net-zero home that most contributes to its low energy consumption is the tight and highly insulated envelope. This tight envelope requires the use of mechanical ventilation to comply with outdoor air ventilation requirements, which, in the summer months, introduces moisture into the space (ASHRAE 2013). This moisture was removed by the HP to hold humidity levels at the 50% RH setpoint. The heat pump operated normally and in the dedicated dehumidification mode to produce a sensible heat ratio (SHR) of approximately 70% (Figure 4b), which was the SHR needed to maintain a 50% indoor RH and support occupant comfort.

EFFECT OF STANDBY ENERGY ON PERFORMANCE

Cooling and heating annual energy efficiency were affected by the HP's standby power demand. Table 4 shows the electrical energy consumed by the heat pump and the percentage of standby time during the cooling and heating modes. Overall the standby energy consumption was 5.2% and 3.5% of the total electrical energy used for cooling and heating, respectively.

Table 4: Standby Energy Use

Cooling Standby Energy (kWh) and Percentage of Time in Standby Mode

Jul-2013	Aug-2013	Sep-2013	Oct-2013	Apr-2014	May-2014	Jun-2014
12.6, 34%	17.2, 46%	23.4, 64%	25.6, 87%	3.1, 99%	30.5, 82%	16.2, 45%

128.6 kWh standby cooling, 5.2% of total cooling electrical energy

Heating Standby Energy (kWh) and Percentage of Time in Standby Mode

Oct-2013	Nov-2013	Dec-2013	Jan-2014	Feb-2014	Mar-2014	Apr-2014
6.8, 98%	25.2, 72%	21.3, 59%	14.3, 38%	14.9, 45%	21.5, 59%	29.4, 93%

133.2 kWh, 3.5% of total heating electrical energy

HEAT RECOVERY VENTILATOR IMPACT

Ventilating the house using an HRV resulted in a 7% savings in heat pump energy use on average over the year compared with ventilating without heat recovery. The impact on the heat pump energy use ranged from a 5% increase in cooling months to a 36% savings in heating months (Figure 5). However, in this climate, the annual savings in heat pump energy were offset by the increased power consumption of the HRV compared to a supply fan without heat recovery. These findings are consistent with the literature studies, which were conducted using simulations (Rudd et al. 2013).

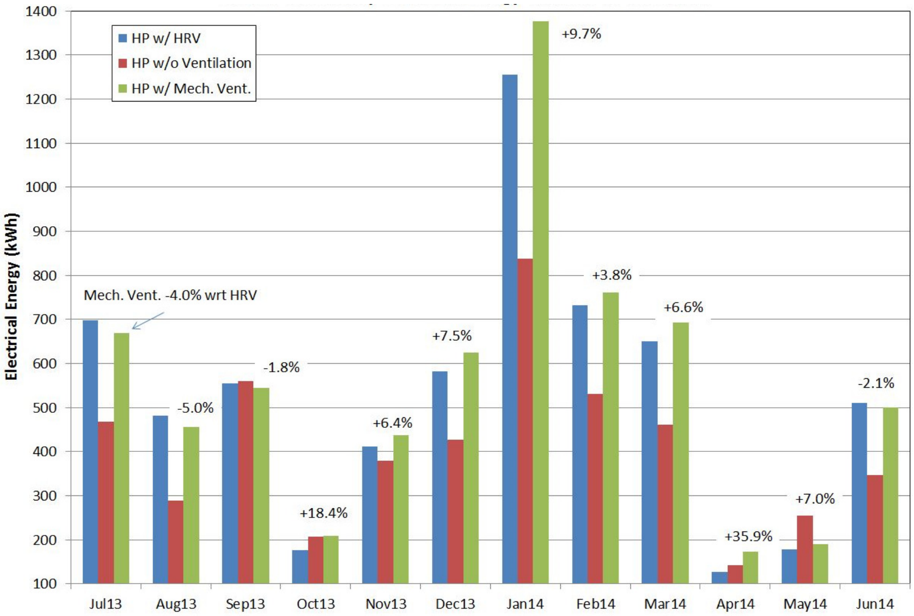


Figure 5 Heat pump electrical energy use due to mechanical ventilation.

HOUSE AND HEAT PUMP PERFORMANCE SUMMARY

During the first year of operation, the home's annual energy consumption was 13 039 kWh (4.8 kWh ft^{-2} or 51.7 kWh m^{-2}), and the 10.2 kW solar PV generated an excess of 484 kWh. The HP consumed a total of 6225 kWh (2442 kWh cooling, 3783 kWh heating) of electrical energy while transferring a total of 14 924 kWh of thermal energy (7217 kWh cooling, 7707 kWh heating) between the indoor space and outdoor environment (combined EER of 8.18 Btu W^{-1}h^{-1}, COP of 2.40 W W^{-1}). The heat pump operated for a total time of 3503 h (1785 h cooling, 1718 h heating) or 40% of the year. For the majority of the time, the heat pump was in standby mode, which consumed a total of 262 kWh (129 kWh cooling, 133 kWh heating) or 2% of the total site electrical energy consumption. Supplemental dehumidification was required to maintain a "comfortable" 50% RH at all times; this supplemental dehumidification used 892 kWh or 14.3% of the heat pump's energy use or 6.8% of the entire site electrical energy. The heat pump's resistive heat electrical energy used totaled 1157 kWh of which 352 kWh was consumed during defrost and 805 kWh was consumed for direct supplemental heating. Resistive heat for supplemental heating was 12.9% of the heat pumps total electrical energy use or 6.2% of the total site electrical energy use.

The original thermostat's control logic would not allow enough time for the heat pump to reach the setpoint in heating mode even when it was capable of increasing the indoor temperature without the resistive heat. A different thermostat with more control options could have saved more than 6% of the total site electrical energy because there were no conditions severe enough to prevent the heat pump from satisfying the heating setpoint.

Human comfort and maximum heat pump SEER are at odds with each other. An air-conditioning system should be designed to efficiently provide comfort in its specific climate zone; therefore, maximum possible SEER will vary with climate zone just as average daily outdoor humidity varies with climate zone. Heat pumps and air conditioners, with their controls, should be rated for dehumidification performance by a non-burdensome laboratory test method.

NOMENCLATURE

AC = Air-Conditioner

cfm = cubic feet per minute, ft^3 min^{-1}

COP= Coefficient of Performance, W W^{-1}

DC = Direct Current

EER = Energy Efficiency Ratio, Btu W^{-1} h^{-1}

HP = Heat Pump

HRV = Heat Recovery Ventilator

HSPF = Heating Seasonal Performance Factor, Btu W^{-1} h^{-1}

HVAC = Heating, Ventilating, and Air-Conditioning

NZE(H) = Net-Zero Energy (Home)

NZERTF = Net-Zero Energy Residential Test Facility

PV = Photovoltaic

SEER = Seasonal Energy Efficiency Ratio, Btu W^{-1} h^{-1}

ZEH = Zero Energy Home

ACKNOWLEDGEMENTS

The author would like to acknowledge the contributions of Hunter Fanney, Lisa Ng, Brian Dougherty, Joshua Kneifel, Tania Ullah, Farhad Omar, Matthew Boyd, Luis Luyo, John Wamsley, and Arthur Ellison (all of NIST) in contributing to the content and measurements needed to produce this paper.

REFERENCES

AHRI, 2008, Standard 210/240: Performance Rating of Unitary Air-Conditioning and Air-Source Heat Pump Equipment, Air-Conditioning, Heating, and Refrigeration Institute. http://www.ahrinet.org

ASHRAE. 2013. “Standard 62.2-2013: Ventilation and Acceptable Indoor Air Quality in Low-Rise Residential Buildings”. ASHRAE, USA.

Davis M., Healy W., M. Boyd M., Ng L., Payne V., Skye H., Ullah T., 2014, Monitoring Techniques for the Net-Zero Energy Residential Test Facility, NIST Technical Note 1854, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=917208.

DOE 2010, Building Energy Data Book, U.S. Department of Energy. [Web page], http://buildingsdatabook.eren.doe.gov/

EPA, 2015, Dehumidifiers Key Efficiency Criteria, http://www.energystar.gov/index.cfm?c=dehumid.pr_crit_dehumidifiers accessed July 17, 2015

Kneifel J., 2012, Annual Whole Building Energy Simulation of the NIST Net Zero Energy Residential Test Facility Design, NIST Technical Note 1767, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912187.

Musall E., T. Weiss, K. Voss, A. Lenoir, M. Donn, S. Cory, and F. Garde, 2010, Net Zero Energy Solar Buildings: An Overview and Analysis on Worldwide Building Projects, in Proceedings of 2010 Eurosun Conference, Int. Conf. on Solar Heating Cooling and Buildings, Graz, Styria, Austria.

Omar F., S. Bushby, 2013, Simulating Occupancy in the NIST Net-Zero Energy Residential Test Facility, NIST Technical Note 1817, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=914650.

Parker D. S., 2009, Very low energy homes in the United States: Perspectives on performance from measured data, Energy and Buildings, 41 (5), 512-520.

Petit B., Gates C., Fanney A. H., and Healy W. M., 2015, Design Challenges of the NIST Net Zero Energy Residential Test Facility, NIST Technical Note 1847, http://dx.doi.org/10.6028/NIST.TN.1847.

Rudd A., H. I. Henderson, D. Bergey, and D. B. Shirey, 2013, ASHRAE 1449-RP: Energy Efficiency and Cost Assessment of Humidity Control Options for Residential Buildings, ASHRAE 1449-RP Final Report, Atlanta, GA, 204 pp.

Rudd A., 2014, Measure Guideline: Supplemental Dehumidification in Warm-Humid Climates, Building America Program Report, http://www.osti.gov/scitech.

Sherwin J., C. Colon, D. Parker, and E. Martin, 2010, Performance of Four Near Zero Energy Homes: Lessons Learned, in Thermal Performance of the Exterior Envelopes of Whole Buildings XI, . December 5-9, 2010, Clearwater Beach, Florida, ISBN: 978-1-933742-89-2.

Improved spectral aberration in Johnson Noise Thermometry

A. Pollarolo[1], H. Rogalla [1, 2], A. Fox[1], K. J. Coakley[1], W. L. Tew[3], S. P. Benz[1]
[1]National Institute of Standards and Technology, Boulder, CO, USA
alessio.pollarolo@nist.gov

[2]ECEE Department, University of Colorado at Boulder, Boulder, CO, USA
[3]National Institute of Standards and Technology, Gaithersburg, MD, USA

***Abstract* — Spectral aberration has been the main source of uncertainty in Johnson Noise Thermometry approach to measuring the Boltzmann constant. Recently, with newly developed hardware and the introduction of a novel fitting algorithm for analyzing the data, we have achieved a frequency independent spectral aberration for measurements with the NIST JNT system. Consequently, we performed a data drift analysis and an electromagnetic interference investigation to explain a residual offset that affects the Boltzmann constant.**

***Index Terms* — Boltzmann equation, Josephson junction, measurement units, noise measurement, standards, temperature measurement.**

I. Introduction

Johnson noise is the thermal fluctuation of the electrons in an electrical resistor. The Nyquist relation describes this phenomenon such that the time-averaged mean-square voltage $\langle V^2\rangle$ across a resistance R is

$$\langle V^2\rangle = 4kTR\Delta f. \tag{1}$$

Here k is the Boltzmann constant, T is the resistor temperature, and Δf is the measurement bandwidth.

Since 2002, NIST has been operating and developing Johnson Noise Thermometry systems based on a Quantum Voltage Noise Source (QVNS) [1]. These systems allow a direct electronic method to determine the Boltzmann constant when they are optimized to measure the noise of a sense resistor at the triple point of water (TPW).

A cross-correlation measurement is necessary to minimize the effect of uncorrelated noise due to voltage amplifiers. The voltage noise of each source, namely, the QVNS and the sense resistor, is alternatively measured for 100 s with two low-noise amplifier channels, from which is calculated the auto- and cross-correlation.

II. Fitting Selection Model

The major system limitation has been the bandwidth dependence of the ratio of the measured power spectral density of the two noise sources. For comparison, we calculate the “offset” ($a_0 - a_{0\text{calc}}$), which correspond to the k, for different bandwidths, namely, the difference of the a_0 intercept of the cross-correlation ratio of the spectral density of the two noise sources (after fitting over a chosen bandwidth) from the calculated value.

Recently, we introduced a new approach to determine the Boltzmann constant based on a cross-validation method [2]. The cross-correlation ratio is fit with an even polynomial function whose complexity (polynomial order) is selected after determining whether the given model is consistent with validation data and training data. The model selection algorithm determines the optimum model or order as a function of the fitting bandwidth. This method was applied to various data sets that were obtained under different conditions.

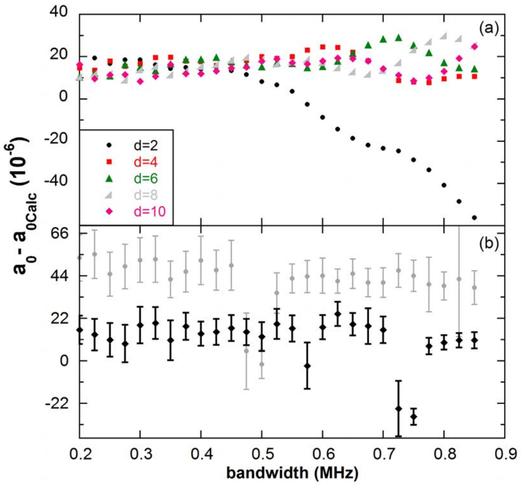


Fig. 1. Cross-correlation ratio fitting. (a) Spectral aberration obtained with higher order “d” polynomials as a function of measurement bandwidth for data “set 2”. (b) Model selection results for an older data “set 1” (gray) and the newest data “set 2” (black).

In Fig. 1, we report the results of the method applied to our newest data “set 2,” which was optimally obtained under stable conditions and in a low electromagnetic interference (EMI) environment, whereas “set 1” was obtain in a common laboratory. Fig. 1(a) reports the offsets vs. different bandwidths that were obtained for five different models with fixed complexity. Fig. 1(b) shows for old and new data sets the selected offsets for different bandwidths that were determined using the model selection algorithm Thanks to hardware improvements [3] and the new model selection method, we achieved (“set 2”) for the first time nearly bandwidth independent results between 200 kHz and 700 kHz for the determination of k, given the reported uncertainty.

III. Data Drift and EMI Investigation

In order to search for systematic errors, we applied the model selection method to the daily single measurements that made up the above data set and fixed the analysis bandwidth

U.S. Government work not protected by U.S. copyright

Pollarolo, Alessio; Rogalla, Horst; Fox, Anna; Coakley, Kevin; Tew, Weston; Benz, Samuel.
“Improved spectra aberration in the Johnson Noise Thermometry.”
Paper presented at the CPEM 2016 Conference, Ottawa, Canada, Jul 10-Jul 15, 2016.
SP-741

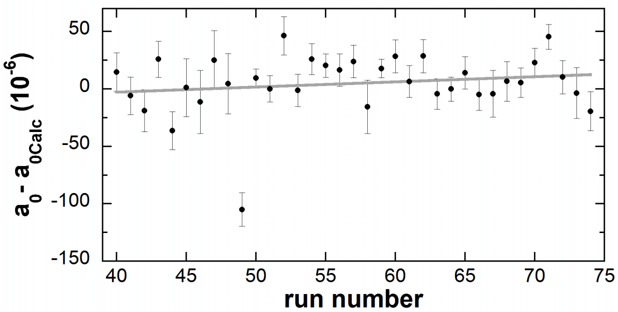


Fig. 2. Values of a_0-a_{0Calc} as function of measurement number or day (black) and the linear trend (gray).

to 850 kHz. Fig. 2 shows the resulting offsets for each day and the linear fit that shows a small upward trend. The line was obtained with a weighted least-squares fit and its uncertainty was estimated with a parametric bootstrap method. The resulting confidence interval for the slope is (0.42 ± 0.16) parts in 10^6 per measurement. Even though this effect does not appear to limit our present measurement, it may become more significant for larger data sets.

Another important feature shown in Fig. 1 (b) is the (a_0-a_{0Calc}) offset reduction between data "set 1" and data "set 2", which is most likely due to the magnitude of EMI coupling to the system. The 18 ppm offset of data "set 2" is likely caused by residual EMI. Even though most of the JNT apparatus resides within the shielded room during the acquisition of data "set 2," the bit code generator (BCG) remains outside the room in order to reduce high frequency EMI. The BCG is connected to the QVNS probe head through coaxial cables, which are brought into the room via a feed-through port.

In order to measure residual EMI coupling to the system, we performed several zero-connection measurements and also examined EMI behavior with two new QVNS chips. The new chips were made so as to provide flexible grounding options and better operating margins. Each chip has two arrays of ten Nb Josephson junctions with Nb_xSi_{1-x} barriers. The new chips incorporate inner-outer DC blocks on the microwave bias lines to each array. The two different chip versions have DC blocks with cut-off frequencies of either 250 MHz or 380 MHz.

During the EMI measurements the grounding connections were maintained in the same configuration as for data "set 2," the QVNS pulse bias was turned off, and the sense resistor was rewired to produce only uncorrelated noise. The uncorrelated noise produced by both noise sources is due to the 200 Ω matching resistors [4]. Since the matching resistors for the QVNS are at 4 K, while those for the sense resistor are at 273.16 K, the integration time for the sense resistor EMI acquisition must be about nine times longer than that of the QVNS in order to achieve the same EMI signal to noise.

Fig. 3 shows the zero-connection cross-correlated power spectral density for the two noise sources. EMI signals are visible at 420 kHz and 840 kHz. In order to eliminate gain effects, the mean and the standard deviation of the mean for both signals was calculated and normalized to the auto-correlations of the two channels. For the sense resistor we obtain a mean and relative uncertainty of (-7.4 ± 0.9) parts in 10^6 when normalizing the data to the ChA auto-correlation and (-7.7 ± 0.9) normalized to ChB. For the QVNS we have (-5.9 ± 2.5) parts in 10^6 and (-7.4 ± 0.9) parts in 10^6, normalized to ChA and ChB, respectively. These results, which are not yet well understood, are still under investigation.

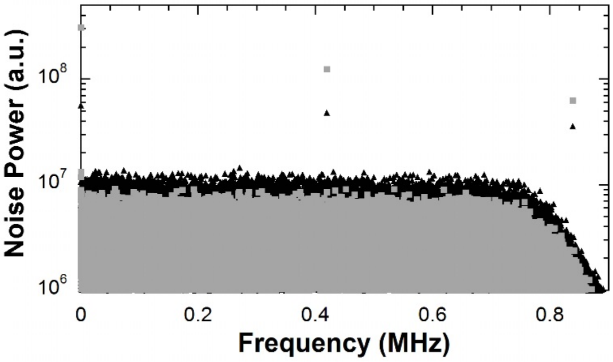


Fig. 3. Cross-correlated measured noise power spectra for the sense resistor (black) and QVNS (gray) vs. frequency. The higher points represent two EMI tones coupling to the apparatus.

VI. Conclusion

Frequency independent (a_0-a_{0Calc}) was demonstrated through a combination of new hardware and a new fitting model selection method. Preliminary EMI measurements were shown that may potentially explain the remaining offset of data "set 2," which is still under analysis.

Acknowledgement

We thank John Kitching and the Time and Frequency Division for allowing us to use the shielded room for these measurements, and Paul Dresselhaus, Nathan Flower-Jacobs and Alain Rufenacht for fruitful collaborations.

References

[1] S. P. Benz, J. M. Martinis, S. W. Nam, W. L. Tew, and D. R. White, "A new approach to Johnson noise thermometry using a Josephson quantized voltage source for calibration," *Proceedings of TEMPMEKO 2001, the 8th International Symposium on Temperature and Thermal Measurements in Industry and Science*, B. Fellmuth, J. Seidel, and G. Scholz, Eds., Berlin: VDE Verlag, vol. 19, pp. 37-44, April 2002.

[2] K. J. Coakley and J. Qu, "Selection of spectral distortion model for electronic determination of the Boltzmann constant," in preparation.

[3] A. Pollarolo, H. Rogalla, W. Tew, K. Coakley, and S. P. Benz "2 channels system for Boltzmann constant determination based on Johnson noise thermometry", in preparation.

[4] A. Pollarolo, *T. Jeong, S. P. Benz, H. Rogalla*, "Johnson noise thermometry measurement of the Boltzmann constant with a 200 Ω sense resistor", *IEEE Trans. Instrum. Meas.,* vol. 62, pp. 1512-1517, May 2013.

"Improved spectra aberration in the Johnson Noise Thermometry."

Characterizing Uncertainty of a Formaldehyde Reference Standard

Dustin Poppendieck

Engineering Laboratory, National Institute of Standards and Technology
100 Bureau Drive Gaithersburg, MD 20899

Content submitted to and published by:
Healthy Building 2015 Conference

U.S. Department of Commerce
Penny Pritzker, Secretary of Commerce

National Institute of Standards and Technology
Willie E May, Director

SP-743

Poppendieck, Dustin.
"Characterizing Uncertainty of a Formaldehyde Reference Standard."
Paper presented at the Healthy Buildings 2015 Conference, Boulder, CO, Jul 19-Jul 22, 2015.

DISCLAIMERS

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Any link(s) to website(s) in this document have been provided because they may have information of interest to our readers. NIST does not necessarily endorse the views expressed or the facts presented on these sites. Further, NIST does not endorse any commercial products that may be advertised or available on these sites.

SP-744

Poppendieck, Dustin.
“Characterizing Uncertainty of a Formaldehyde Reference Standard.”
Paper presented at the Healthy Buildings 2015 Conference, Boulder, CO, Jul 19-Jul 22, 2015.

CHARACTERIZING UNCERTAINTY OF A FORMALDEHYDE REFERENCE STANDARD

Dustin POPPENDIECK[1,*]

[1]Indoor Air Quality and Ventilation Group, Engineering Laboratory, 100 Bureau Drive, Mail Stop 8633, Gaithersburg, MD 20899-8633

[*]Corresponding email: dustin.poppendieck@nist.gov

Keywords: Chamber testing, formaldehyde, reference standard

SUMMARY

High performance buildings need to be energy efficient and provide adequate ventilation for indoor air quality, which can be made easier with low emitting building materials. Based in part on these motivations, the United States Environmental Protection Agency (EPA) issued a proposed rule to implement statutory formaldehyde emission standards for hardwood plywood, medium density fiberboard, and particle board products. A Formaldehyde Reference Standard (FRS) is being developed by the National Institute of Standards and Technology (NIST) to assist the implementation of this rule. The goal of this effort is to produce a FRS with small, stable level of uncertainty that can be used in emission chamber system evaluation and troubleshooting. This presentation will highlight uncertainty quantification from preliminary testing of the proposed NIST FRS to begin in February 2015.

INTRODUCTION

High performance buildings need to balance energy efficiency and providing adequate ventilation for indoor air quality. The level of required ventilation can potentially be reduced when low emitting building materials are used. The United States Environmental Protection Agency (EPA) issued a proposed rule to implement statutory formaldehyde emission standards for hardwood plywood, medium density fiberboard, and particle board products. The proposed rule requires formaldehyde emission chamber testing of various wood products and third-party certification of emission testing. A Formaldehyde Reference Standard (FRS) is being developed by the National Institute of Standards and Technology (NIST) to assist implementation of this rule. The intent of the FRS is to assist in evaluating chamber testing performance and support the small chamber/large chamber equivalency requirements in the proposed EPA rule and the existing California Air Resources Board (CARB) Airborne Toxic Control Measure (ATCM) to Reduce Formaldehyde Emissions from Composite Wood Products. Previous interlaboratory testing of standard wood products has shown large variability (e.g. 20 % standard deviations, Yrieix 2010). The goal of this effort is to produce a FRS with small, stable level of uncertainty that can be used in emission chamber system evaluation and troubleshooting.

This presentation will highlight uncertainty quantification from preliminary testing of the proposed NIST FRS. All measurements related to chamber testing (formaldehyde concentration, temperature, relative humidity, flow and pressure) will be traceable to NIST primary standards. The experiments will be conducted in the spring of 2015; this abstract reviews the methods to be used.

Poppendieck, Dustin.
"Characterizing Uncertainty of a Formaldehyde Reference Standard."
Paper presented at the Healthy Buildings 2015 Conference, Boulder, CO, Jul 19-Jul 22, 2015.

METHODOLOGIES

Experiments will be conducted following ASTM D6007-02 (2008) (Standard Test Method for Determining Formaldehyde Concentrations in Air from Wood Products Using a Small-Scale Chamber) as closely as possible. In this method, small samples of wood are introduced into a climate-controlled chamber (0.02 m^3 to 1 m^3 volume, 0.5/h air change rate, 25 °C ± 1 °C temperature and 50 % ± 4 % relative humidity) at a standard loading ratio. Formaldehyde concentrations are measured once the chamber has reached equilibrium and emission rates are calculated. This work will deviate from ASTM D6007 in the following ways:

- The tested material is a formaldehyde-water solution contained in a small bottle (as described below) instead of a wood sample.
- The samples will be analyzed using a quantum cascade laser trace gas monitor. This instrument provides real time data with standard uncertainties of the measurements less than 0.1 ppb_v (0.13 $\mu g/m^3$), making it advantageous compared to the chromotropic acid test procedure described in D6007.

Experiments to test the formaldehyde reference standard will be conducted in the NIST small chamber system. Only one 50 L chamber will be used in this research. A zero air generator will supply formaldehyde free air to the chamber. To achieve the desired relative humidity (50 %), humidified and dry air streams will be mixed in a controlled fashion using two mass flow controllers (MFC).

Each experiment will consist of placing a formalin-containing Teflon and stainless steel bottle in the chamber (Figure 1). This design is based on work done by Wei et. al. (2013). The 1 mL ampules of 16 % formalin solution (mass of formaldehyde/volume of distilled deionized water) will be acquired from an outside manufacturer.

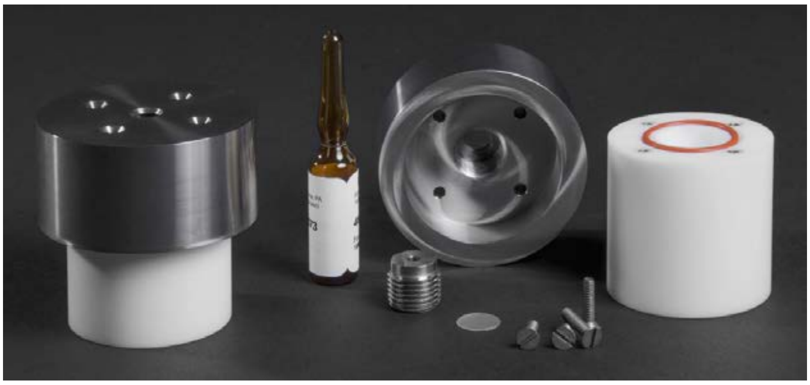


Figure 1: NIST formaldehyde reference standard (FRS). The FRS consists of a formalin ampule, a stainless steel lid, a compression set screw, a polydimethylsiloxane (PDMS) membrane, four stainless steel screws, a Teflon base with 3 mL formalin well, and an o-ring. The lid is sealed to the bottle with the screws.

Formaldehyde from the FRS will diffuse through a thin polydimethylsiloxane (PDMS, 1.0 mm) membrane, eventually reaching a steady state formaldehyde concentration in the chamber. The target steady state formaldehyde concentration is between 20 and 50 ppb_v (25 $\mu g/m^3$ and 63 $\mu g/m^3$). The key component of the FRS is the replaceable membrane. Each time the FRS is used a new membrane and new formalin solution will be placed in the bottle. Formaldehyde concentrations will be measured using a quantum cascade laser trace gas monitor. Given the known absorption spectra for each of the known constituents, the measured spectra can be deconvoluted to determine the concentration of the formaldehyde, formic acid and water in the sample. Currently experiments are planned to be run until the formaldehyde concentration reaches a value that does not change more than 2 % over six hours. Ten bottles have been manufactured in this first phase of the project. Initially a random selection of five of these bottles will be tested twice. Each replicate experiment of each bottle will use a new membrane and new formalin ampule. These initial data will be used to confirm that the uncertainty of the emission rate is within acceptable bounds.

Measurement Equation

The chamber system's small mixing fan produces a uniform contaminant concentration. Hence, the emission rate of the FRS will be determined using a single-zone mass balance approach. The formalin concentration in the bottle should remain relatively constant for the duration of the experiment, resulting a steady-state diffusion across the membrane. This constant emission rate will result in the chamber reaching a steady state formaldehyde concentration. The emission rate can be determined as follows:

$$E = Q(C - C_{in}) \tag{1}$$

Where E is the emission rate (μg/h), Q is the total flow rate (m^3/h), C is the formaldehyde concentration in the chamber (μg/m^3) and C_{in} is the formaldehyde concentration entering the chamber from sources other than the formaldehyde diffusing out of the bottle (μg/m^3, which should be zero).

Uncertainty in the emission rate will be quantified using the "Evaluation of measurement data — Guide to the expression of uncertainty in measurement" (JCGM 2008). This approach assumes that measurement uncertainty "reflects the lack of exact knowledge of the value" of the emission rate. Uncertainty is "best described by means of a probability distribution over the set of possible values" for the emission rate. To determine the probability distribution for the value of the emission rate, a range of factors that could influence the measured value must be considered. The emission rate is expected to depend on a range of factors including temperature, relative humidity, pressure, flow, exposed membrane area, membrane thickness, and formalin concentration. The first four factors are set points for the experimental system and may have a systematic impact on the emission rate. The last three factors will impact the emission rate in a random manner. Random variation in exposed membrane area, membrane thickness, and formalin concentration will be captured in the standard uncertainty of the emission rate. (Any instability in the values of the set point factors that lead to variations in the data will be included in these standard uncertainties as well.) Systematic errors will not be captured in the standard uncertainty values for flow and concentration. Hence, systematic errors need to be included in the uncertainty in another manner. The measurement equation used to determine the expanded uncertainty is:

$$E = Q(C - C_{in}) * f_{temperature} * f_{relative\ humidity} * f_{pressure} * f_{HCHO\ monitor} * \\ f_{flow\ rate}\,\text{dry} * f_{flow\ rate}\,\text{wet} \tag{2}$$

Where f values are the influence quantities, which have a value of 1 for computation of the emission rate and a standard uncertainty determined via calibration of the measurement instruments to NIST primary standard reference values. Influence quantities are not required in the definition of the measurand (E in this case) but do have an effect on the measurement result through their contributions to the uncertainty.

The standard uncertainty in flow (Q) and concentration (C-C_{in}) will be quantified using standard deviations of the flow and concentration data, respectively. The relative contributions to the total variation seen between bottles, between membranes and ampules, and within each bottle, membrane, and ampule will all be considered as part of the assessment of the standard uncertainty of the emission rate. The standard uncertainties of the values of the influence factors will be calculated from the uncertainty comparison between the measured parameter and the relevant NIST primary standard. For example the uncertainty for the influence factor for the formaldehyde monitor will be determined from the variation seen in comparisons between the concentration values from the formaldehyde monitor and the NIST primary gravimetric standard formaldehyde reference source.

The uncertainty in the emission rate will be quantified using the measurement equation (2). A first-order Taylor series expansion with n=1 can be used to determine a linear approximation for the measurement equation near the value of the measurand. The Taylor series then can be used to determine the propagation of uncertainties to determine the combined standard uncertainty. The expanded uncertainty will be calculated from the combined standard uncertainty using a coverage factor of two.

RESULTS AND DISCUSSION

Experiments will commence in February 2015 and complete by June 2015. A summary of the data will be presented at the conference.

In order to develop an acceptable NIST standard reference material based on the FRS approach, additional tests will need to be conducted if the uncertainty from these preliminary experiments is deemed acceptable. Further testing will include testing of a subset of production bottles, membranes and formalin. In addition, a subset will be tested to determine stability of the system after 6 and 12 months. After stability has been confirmed and the final uncertainty deemed acceptable, untested production bottles may be certified and sold.

CONCLUSIONS

Confidence in testing results is needed if emission data are to be submitted to regulatory agencies or is used to meet voluntary product labelling standards. Verification of formaldehyde emission testing data are of particular interest, and therefore merit a reference standard with small, stable level uncertainty. This research will determine if the proposed NIST FRS will have acceptable uncertainty to serve as a verification tool.

ACKNOWLEDGEMENT

Funded in part by EPA Interagency Agreement Number DW-13-92388501-1.

REFERENCES

Evaluation of measurement data — Guide to the expression of uncertainty in measurement. JCGM 100:2008 GUM 1995 with minor corrections: Joint Committee for Guides in Metrology; 2008.

Yrieix, C.; A. Dulaurent; C. Laffargue; F.; Maupetit; T. Pacary, and E. Uhde. (2010). Characterization of VOC and formaldehyde emissions from a wood based panel: Results from an inter-laboratory comparison. Chemosphere 79: 414–419. doi:10.1016/j.chemosphere.2010.01.062

Wei, W.; C. Howard-Reed; A. Persily; Y. Zhang. (2013). "Standard formaldehyde source for chamber testing of material emissions: model development, experimental evaluation, and impacts of environmental factors." Environ Sci Technol 47(14): 7848-7854.

Formaldehyde Concentrations in a Net-Zero Energy House: Real-time Monitoring and Simulation

Dustin Poppendieck
Shahana Khurshid
William Dols
Lisa Ng
Brian Polidoro
Steven Emmerich

Engineering Laboratory, National Institute of Standards and Technology
100 Bureau Drive Gaithersburg, MD 20899

Content submitted to and published by:
14th International Conference on Indoor Air Quality and Climate Conference

U.S. Department of Commerce
Penny Pritzker, Secretary of Commerce

National Institute of Standards and Technology
Willie E May, Director

SP-749

Poppendieck, Dustin; Khurshid, Shahana; Dols, William; Ng, Lisa; Polidoro, Brian; Emmerich, Steven.
"Formaldehyde Concentrations in a Net-Zero Energy House: Real-time itoring and Simulation."
Paper presented at the International Conference on Indoor Air Quality and Climate Conference, Ghent, Belgium, Jul 3-Jul 8, 2016.

DISCLAIMERS

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Any link(s) to website(s) in this document have been provided because they may have information of interest to our readers. NIST does not necessarily endorse the views expressed or the facts presented on these sites. Further, NIST does not endorse any commercial products that may be advertised or available on these sites.

Poppendieck, Dustin; Khurshid, Shahana; Dols, William; Ng, Lisa; Polidoro, Brian; Emmerich, Steven.
“Formaldehyde Concentrations in a Net-Zero Energy House: Real-time itoring and Simulation.”
Paper presented at the International Conference on Indoor Air Quality and Climate Conference, Ghent, Belgium, Jul 3-Jul 8, 2016.

Formaldehyde Concentrations in a Net-Zero Energy House: Real-time Monitoring and Simulation

Dustin Poppendieck[1,*], Shahana Khurshid[1], W. Stuart Dols[1], Lisa Ng[1], Brian Polidoro[1], Steve Emmerich[1]

[1]Indoor Air Quality and Ventilation Group, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8633, Gaithersburg, MD 20899-8633, USA
[*]*Corresponding email: dustin.poppendieck@nist.gov*

SUMMARY

Measured real-time formaldehyde concentrations in a net-zero energy house were compared to simulated concentrations from a recently-developed, coupled building energy and airflow/indoor air quality model. Measured and simulated formaldehyde concentrations in living spaces ranged from 4 ppb$_v$ to 10 ppb$_v$ (5 μg/m^3 to 12 μg/m^3) while concentrations in the conditioned attic ranged from 13 ppb$_v$ to 28 ppb$_v$ (16 μg/m^3 to 34 μg/m^3). During the 15 minutes the heat recovery ventilator was off each hour, the measured concentration in a bedroom increased by 1 ppb$_v$ (1.2 μg/m^3). In addition, year-long simulations suggest the formaldehyde concentration in the attic may reach almost 50 ppb$_v$ (62 μg/m^3) during the summer. These results highlight the need for source control and effective ventilation (both outdoor air and air distribution) to reduce the concentration of indoor pollutants, particularly in tighter buildings. This research reaffirms the need to consider buildings as multizone systems and provide adequate ventilation to all building zones, particularly those with low outdoor air change rates.

PRACTICAL IMPLICATIONS

Proper mechanical ventilation is increasingly important as new buildings are constructed with or retrofitted to have lower infiltration rates to conserve energy. Without adequate ventilation, indoor pollutant concentrations can exceed levels of concern even in buildings built with low emitting construction materials.

KEYWORDS

Formaldehyde, Net-zero, Model, CONTAM, TRNSYS

1 INTRODUCTION

Formaldehyde is a known human carcinogen (IARC 2012) and exposure to elevated levels of formaldehyde has been linked with a higher incidence of certain types of cancer in cohort studies. Formaldehyde and formaldehyde-based resins are used in the manufacture of particleboard, plywood, paper products, insulation foam, flame resistant fabric, as well as to mold plastic parts for home appliances and consumer products (WHO 2010). Formaldehyde can be emitted from hydrolysis of formaldehyde-based resins (Salthammer et al. 2010). Its widespread use in man-made products is a major source of formaldehyde indoors. Formaldehyde can also be a by-product of combustion. Secondary formation of formaldehyde can occur through the oxidation of alkenes (especially terpenes) as demonstrated in chamber studies (Singer et al. 2006, Waring et al. 2008).

The World Health Organization (WHO) has set a short-term (30 minute) guideline for formaldehyde exposure of 100 μg/m^3 (81 ppb$_v$) to prevent sensory irritation as well as long-term health effects, including nasopharyngeal cancer and myeloid leukemia (WHO 2010). In

Poppendieck, Dustin; Khurshid, Shahana; Dols, William; Ng, Lisa; Polidoro, Brian; Emmerich, Steven.
"Formaldehyde Concentrations in a Net-Zero Energy House: Real-time itoring and Simulation."
Paper presented at the International Conference on Indoor Air Quality and Climate Conference, Ghent, Belgium, Jul 3-Jul 8, 2016.

comparison, the California Office of Environmental Health Hazard Assessment has set a chronic reference exposure limit (REL) for formaldehyde of 9 μg/m^3 (7 ppb$_v$,) (OEHHA 2014). This REL is the concentration at which adverse noncancer health effects are not expected for continuous chronic exposures.

Whether a formaldehyde health standard is exceeded in an indoor environment is primarily dependent upon source strength (emission, reaction, combustion) and outdoor air change rate. Formaldehyde concentrations will be lower in environments with low source strengths and high air change rates. High performance buildings are typically constructed with low source strength materials but may be designed to operate at low air change rates.

Typically, time-averaged methods (e.g., ASTM D5197-09e1) have been used to measure formaldehyde concentrations using derivatizing agent-filled sorbent tubes that are sampled over periods lasting several hours or even days. These methods do not capture variations in concentration at the time scales (seconds to hours) required to understand transient effects such as indoor chemistry that results in formaldehyde formation or the impacts of space conditioning equipment operation. To date, limited knowledge exists of the dynamic nature of indoor formaldehyde concentrations. Most of the research on the influence of environmental conditions (such as temperature and relative humidity) on formaldehyde concentrations has been limited to chamber studies. Measuring real-time, high resolution formaldehyde concentrations is vital to understanding the emission of formaldehyde from building materials, its formation from indoor chemical reactions and the impacts of equipment operation. Measuring real-time indoor concentrations of formaldehyde also allows for the verification of simulation models of indoor formaldehyde concentrations.

Real-time monitoring of indoor ambient formaldehyde concentrations has been limited to Fourier Transform Infrared (FTIR) spectrometry and sensor-spectrophotometric devices. Typically, FTIR spectrometers are limited to a method detection limit (MDL) of about 8 ppb$_v$ (9.8 μg/m^3) for formaldehyde (Wei et al. 2013). A sensor-spectrophotometric device has been shown to have a 2 ppb$_v$ (2.5 μg/m^3) MDL and a sampling cycle of one minute (Carter et al. 2014). Recent advancements in laser spectrometry have led to the development of a real-time formaldehyde monitor that has an MDL of 0.1 ppb$_v$ (0.12 μg/m^3). This instrument was used in this study to measure real-time formaldehyde concentrations in a net-zero energy house and to demonstrate the short term, dynamic impacts of a heat recovery ventilator (HRV) on indoor concentrations. The measured concentrations were also compared to simulation results from a coupled building energy and airflow/contaminant transport model of the house.

2 MATERIALS/METHODS

A net-zero energy test house was monitored in real-time to examine variations in indoor formaldehyde concentrations and to determine if these variations can be captured in models.

Test Facility

The National Institute of Standards and Technology (NIST) constructed the Net-Zero Energy Residential Test Facility (NZERTF) in Maryland, USA in 2012. The facility functions as a laboratory to support the development and adoption of cost-effective net-zero energy (NZE) designs and technologies, construction methods, and building codes. The two-story house with a basement and attic is similar in size (242 m^2 for occupied floors, 485 m^2 inside the building envelope including the attic and basement) and aesthetics to homes in the surrounding communities. The house is not furnished other than permanently installed cabinetry. One key design objective was to provide for occupant health and comfort through adequate ventilation and reduced indoor contaminant sources. For source control, guidelines were implemented to minimize use of products with urea-formaldehyde resin and elevated emissions of volatile organic compounds (VOC). More information on the NZERTF design and long term monitoring of VOC concentrations can be found in Poppendieck, et. al. (2015).

Several technologies are employed in the house to achieve the net-zero energy goals including a 10.2 kW photovoltaic system, a high efficiency air-to-air heat pump, a solar hot water system, and a heat recovery ventilator (HRV). All floors of the house, including the attic, are within the conditioned space. A central heat pump system provides supply air to all floors except the attic. Passive air transfer grilles connect the basement to the first floor and attic to the second floor of the house. Air is returned to the heat pump via two return air grilles located on the first and second floor. A separate HRV system provides air to the first floor kitchen and second floor bedrooms and draws air for heat recovery from three bathrooms located on the first and second floors. To comply with the outdoor air requirements in ASHRAE Standard 62.2-2010 (ASHRAE 2010), the HRV was sized to deliver 137 m^3 h^{-1} of outdoor air, which is equivalent to an air change rate of 0.11 h^{-1}. Tracer tests performed in the summer and winter showed the infiltration through the building envelope to vary between 0.02 h^{-1} to 0.06 h^{-1} when the HRV was off and the total outdoor air change rate (mechanical ventilation plus infiltration) to vary between 0.17 h^{-1} to 0.19 h^{-1} when the HRV was on. (Ng et al. 2015)

Model

Modelling of the NZERTF was performed using the whole-building multizone airflow and indoor air quality software CONTAM (Dols et al. 2015) coupled with the TRaNsient **S**ystems **S**imulation Tool (TRNSYS, (Duffy et al. 2009)) building energy analysis software. CONTAM accounts for the interaction between external driving forces (ambient temperature and wind) and internal mechanisms (building mechanical system airflows) to determine resultant pressures and airflows across internal and external building partitions, i.e., interzone and infiltration/exfiltration airflows. It can then account for external and internal contaminant sources and removal mechanisms to calculate contaminant transport associated with the previously determined airflows. TRNSYS has a modular structure that enables multiple energy-related systems to be considered together within a single simulation environment. Modules are referred to as Types. Type 56 implements a whole-building multizone heat transfer model that can account for conductive, convective and radiant heat transfer associated with building materials (e.g., walls, floors, ceilings and windows); interzone and infiltration airflows; and heating and air-conditioning systems that can be simulated using a wide range of existing and/or user-defined modules.

Both CONTAM and TRNSYS Type 56 have limitations. CONTAM relies on user-defined values for internal temperatures to calculate airflows, while Type 56 requires the input of infiltration and inter-zone airflow rates to calculate temperatures. By coupling these two models, the limitations of each can be overcome. During the simulation, data is exchanged between the two models to form the coupled simulation as described in Dols et al. (2015).

The NZERTF was modelled as a four zone building consisting of one zone for each floor including the basement and attic. Model inputs were determined based on building design and measurements. Ventilation system airflow rates including heat pump supply and return; HRV supply and return; and bathroom, range hood and dryer vent exhaust were measured with a balometer or a duct traverse using a hot wire anemometer. A blower door test was performed to measure the building envelope leakage rate. This envelope leakage was distributed over the entire above-grade building envelope in the CONTAM representation. These measurements and other house properties are provided in Ng et al. (2015) and the TRNSYS representation including the mechanical systems was developed by Leyde (2014) and calibrated with measured data by Balke (2016). Poppendieck, et. al. (2015) previously used a CONTAM-only model to predict infiltration rates by defining all system flows and zone temperatures. In contrast, this coupled model simulated thermostat control of the space conditioning system to establish heat pump operation and calculate zone temperatures.

The average occupied floor area (1st floor and 2nd floor) formaldehyde emission rate over one year (6.7 µg h^{-1} m^{-2}) was measured using one hour 2,4-dinitrophenylhydrazine (DNPH) cartridge sampling according to ASTM D5197 (ASTM 2009) and reported in Poppendieck et. al. (2015). Preliminary investigations indicated that there was likely no significant source of formaldehyde in the basement, but there are potential sources on other levels. The source was modeled as being present in the 1st floor, 2nd floor and attic. Hence, the floor area formaldehyde emission rate (5.1 µg h^{-1} m^{-2}) was normalized to include the attic floor area.

Measurements

A real-time spectrophotometric formaldehyde monitor was placed in the NZERTF for three weeks. The sensitivity of the monitor is 0.1 ppb_v (0.12 µg/m^3) with a one second sampling time. Sampling lines were run from each room to an automatic seven port sampling valve, which fed into the monitor. The monitor recorded the formaldehyde concentration at each location in series for two three-day periods (Session 1 and Session 2). Each location was sampled for two minutes every 15 minutes. The monitor was zeroed every 15 minutes.

Tracer gas decay tests were conducted concurrently with the formaldehyde monitoring. During Session 1 a fan was placed at the top of each stairwell (between basement and 1st floor, and between 1st and 2nd floor) to enhance the mixing of the tracer. During Session 2 a single fan was placed between the 1st and 2nd floor, while the door to the basement was closed. Estimated mixing fan flows were included in the model. Formaldehyde concentrations were similar for floors connected with a mixing fan.

The formaldehyde monitor was also used to individually monitor each of seven locations continuously over day long periods. The monitor recorded data from each location for 12 out of every 15 minutes. The remaining time was used to zero the instrument and record outside concentrations. Relative humidity, temperature and ozone concentrations were separately monitored.

3 RESULTS AND DISCUSSION

The measured formaldehyde concentrations in the 1st floor, 2nd floor, and basement were similar during both measurement sessions (Figure 1). The measured concentrations in the zones ranged from 4 ppb_v to 10 ppb_v (5 µg/m^3 to 12 µg/m^3). These concentrations bracket the OEHHA chronic REL for formaldehyde of 7 ppb_v (9 µg/m^3) (OEHHA, 2015).

The measured formaldehyde concentrations in the attic were two to four times higher than the concentrations in the other zones. The attic in the NZERTF is within the conditioned space, but is only connected to the occupied zone via two passive transfer grills. The tracer decay rate in the attic was two to three times lower than other measured locations in the NZERTF during Session 1. This lower air change rate is consistent with the attic having higher formaldehyde concentrations assuming the equivalent emission rate for all the spaces. In the CONTAM model the formaldehyde emission rate was defined to be evenly distributed throughout the 1st floor, 2nd floor and attic based on floor area. The model data (solid lines in Figure 1) follow the same trends as the measured data, with the attic concentration being two to three times higher than the other zones. Since the model was assigned the same formaldehyde emission value throughout the 1st floor, 2nd floor and attic, this result indicates that the elevated concentrations in the attic are largely due to the reduced ventilation in the attic compared to the other zones in the house.

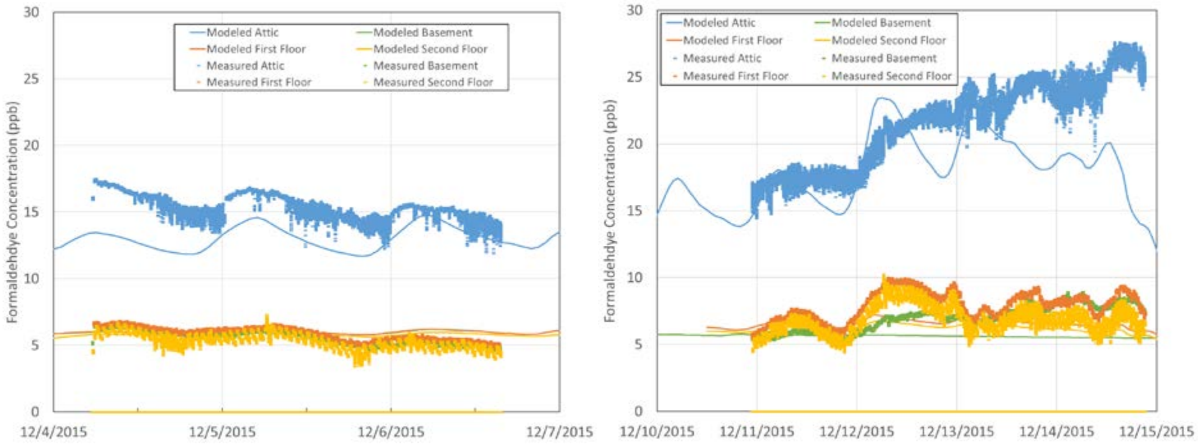


Figure 1. Real time formaldehyde concentration (ppb$_v$) data from two three-day sampling sessions. During Session 1 (left) the average outdoor temperature was 3.5 °C (standard deviation SD=4.4 °C) and the average wind speed was 0.9 m/s (SD = 1.3 m/s). During Session 2 (right), the average outdoor temperature was 12.7 °C (SD = 4.9 °C) and the average wind speed was 0.9 m/s (SD=1.1 m/s)..

The higher average outdoor temperature of 12.7 °C during Session 2 (Figure 1, right) likely resulted in higher formaldehyde concentrations as compared to Session 1 (3.5 °C). The average wind speed was the same for both sessions. As the outdoor temperatures approach indoor temperatures there is a lower driving force for infiltration. Lower infiltration rates should have greater influence on chemical concentrations in zones without direct mechanical ventilation, such as the attic in this house. The modeled emission rates were constant and not adjusted for indoor temperature changes. This indicates that the greater increase in formaldehyde concentrations during Session 2 in the attic compared to the rest of the zones is likely the result of reduced outdoor air change in the attic.

Air mixing within the NZERTF also varied between Session 1 (more mixing) and Session 2 (less mixing). Due to the lower temperatures during Session 1, the heat pump system operated for a longer period of time and resulting in more mixing during Session 1 than Session 2. In addition, during Session 1 a fan was placed at the top of the stairwell between the basement and 1st floor to enhance the mixing of the tracer. During Session 2 the door to the basement was closed. The decrease in mixing in Session 2 led to a greater difference between the measured 1st and 2nd floor concentrations and the basement concentrations (especially on 12/12/15) (Figure 1, right) compared with Session 1 (Figure 1, left).

The measured formaldehyde concentration on the 2nd floor varied to a greater extent than the measured concentration on the 1st floor and basement (Figure 1). To investigate this variation, the formaldehyde concentration was measured in the middle of the 2nd floor master bedroom continuously for one day (Figure 2). The master bedroom was supplied with outside air via the HRV for 40 minutes of every hour (black line Figure 2). Every time the HRV was off the formaldehyde concentration in the room increased 1 ppb$_v$ (1.2 μg/m^3) in roughly 15 minutes. The formaldehyde concentration decreased by a similar amount during the 45 minutes the HRV was supplying outdoor air to the room.

Formaldehyde emissions rates in laboratory settings have been shown to be temperature and relative humidity dependent (Liang et al. 2015). Preliminary observations show that the master bedroom formaldehyde concentration correlated more strongly with the outdoor relatively humidity values (Figure 2), rather than the indoor relatively humidity. No trends were observed between the formaldehyde concentration, ozone concentration, indoor temperature and outdoor temperature. These dependencies will be the subject of future studies at the NZERTF. The collected master bedroom data does show that during the winter, the impact of a 12 % change in outdoor relatively humidity at the NZERTF had a lesser effect on formaldehyde concentrations than turning off the HRV.

The importance of ventilation in high performance buildings is underscored by the fact that (i) a lower air change rate in the NZERTF attic led to elevated formaldehyde concentrations in the attic and (ii) the formaldehyde concentration and the HRV operation in the master bedroom were correlated.

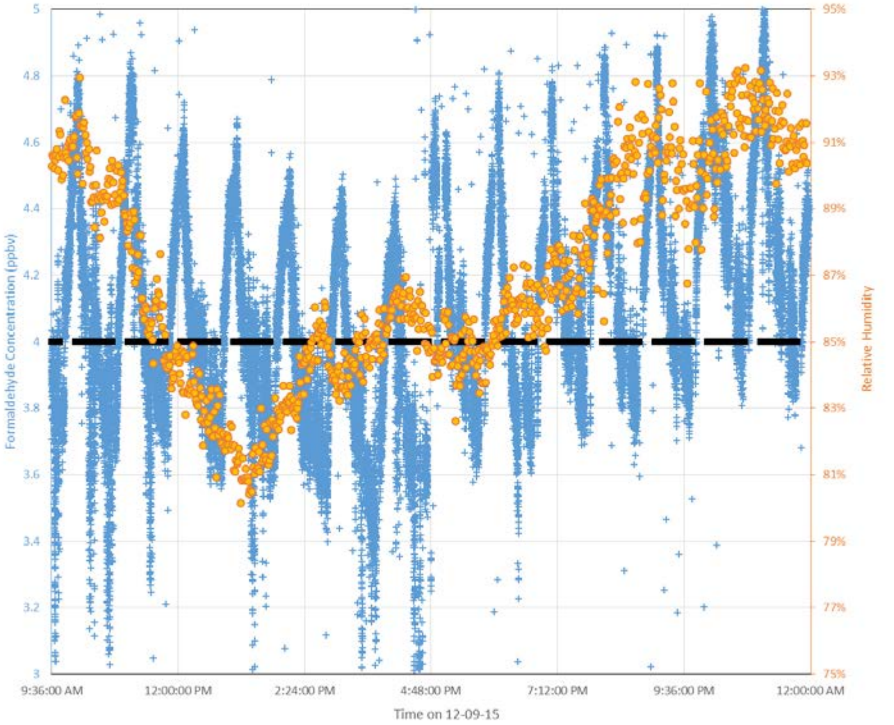


Figure 2. Real-time formaldehyde concentration (ppb$_v$) data from master bedroom. The HRV was on and providing outdoor air to the master bedroom for 40 minutes of every hour, as indicated by solid portion of the black line. The gaps in the black line show when the HRV was off. Blue data points are the formaldehyde concentration (ppb$_v$) and orange data points are the outdoor relative humidity (%).

The model achieved a reasonable, although not exact, agreement with the measured data (Figure 1) taken at the NZERTF. While measurements were made in winter, the model was run for a full year, using 2015 weather data, to assess peak formaldehyde concentrations in the NZERTF (Table 1). During the modelled year, the maximum simulated formaldehyde concentration in the attic was 47 ppb$_v$ (56 μg/m^3), while the maximum simulated formaldehyde concentration in the living space was 9.5 ppb$_v$ (11.7 μg/m^3). The average predicted formaldehyde concentrations in the summer months (June, July and August) were 29 ppb$_v$ (±5.8 ppb$_v$, 36 μg/m^3 ±7.1 μg/m^3) in the attic and 9.5 ppb$_v$ (±0.6 ppb$_v$, 12 μg/m^3 ±0.7 μg/m^3) on the 1st floor.

Table 1. Predicted Formaldehyde Concentrations in the NZERTF over a year of operation (ppb$_v$). Average summer values are from June, July and August.

Zone	**Maximum**	**Summer Average**	**Yearly Average**	**Yearly Standard Deviation**
Attic	47.1	28.0	18.8	6.2
Second Floor	8.7	6.8	5.9	0.8
First Floor	9.5	7.8	7.3	1.0
Basement	8.8	7.4	6.3	1.0

4 CONCLUSIONS

The purpose of the NZERTF is to demonstrate that a typical home can achieve net-zero energy operation while maintaining acceptable indoor environmental conditions. Key design elements of the NZERTF include thermal envelope construction with minimal air leakage and the provision of controlled mechanical ventilation. This research shows that even though the NZERTF meets the ventilation requirements in ASHRAE Standard 62.2 and uses building products with low emission rates, formaldehyde concentrations were elevated during times when the ventilation (HRV) is off and in zones with minimal ventilation air distribution (attic). As new construction seeks to employ these same design principles, specifically low envelope infiltration rates as well as effective and reliable mechanical ventilation, including both adequate outdoor air intake rates and good air distribution are critical for controlling indoor pollutants.

While time-averaged sampling techniques are appropriate for evaluating potential chronic health impacts and have a cost advantage, real-time measurements of formaldehyde concentrations provide new insights to the indoor environment. Real time monitoring of formaldehyde proved to be beneficial for investigating coupling among zones, short term variations in concentrations attributable to mechanical system operation, and associations of concentrations with physical parameters. In addition, the frequent and high-accuracy measurements throughout the NZERTF allowed for verification of a coupled CONTAM and TRNSYS model.

ACKNOWLEDGEMENT

The authors would like to acknowledge the assistance of Dan Greb of National Institute of Standards and Technology in the sampling of formaldehyde concentrations and in conducting the tracer gas tests.

5 REFERENCES

ASHRAE (2010). Standard 62.2-2010: Ventilation and Acceptable Indoor Air Quality in Low-Rise Residential Buildings. Atlanta, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

ASTM (2009). ASTM D5197-09e1, Standard Test Method for Determination of Formaldehyde and Other Carbonyl Compounds in Air (Active Sampler Methodology). West Conshohocken, PA, American Society of Testing and Materials (ASTM) International. **D5197-09e1**.

Balke, E. C. (2016). Modeling, Validation, and Evaluation of the NIST Net Zero Energy Residential Test Facility. M. S., University Of Wisconsin – Madison.

Carter, E. M., M. C. Jackson, L. E. Katz and G. E. Speitel (2014). "A coupled sensor-spectrophotometric device for continuous measurement of formaldehyde in indoor environments." J Expos Sci Environ Epidemiol **24**(3): 305-310.

Dols, W. S., S. J. Emmerich and B. J. Polidoro (2015). "Using coupled energy, airflow and indoor air quality software (TRNSYS/CONTAM) to evaluate building ventilation strategies." Building Services Engineering Research and Technology.

Dols, W. S. and B. J. Polidoro (2015). CONTAM User Guide and Program Documentation. Gaithersburg, MD, National Institute of Standards and Technology.

Duffy, M. J., M. Hiller, D. E. Bradley, W. Keilholz and J. W. Thornton (2009). TRNSYS - Features and Functionalitity for Building Simulation 2009 Conference. 11th International IBPSA Conference - Building Simulation 2009. Glasgow, United kingdom, International Building Performance Simulation Association**:** 1950-1954.

IARC (2012). Chemical Agents and Related Occupations: Volume 100 F A Review of Human Carcinogens. IARC Monographs on the Evaluation of Carcinogenic Risks to Humans. Lyon, France, International Agency for Research on Cancer. **100 F**.

Leyde, B. P. (2014). TRNSYS modeling of the NIST Net Zero Energy Residential Test Facility, University of Wisconsin - Madison.

Liang, W., S. Yang and X. Yang (2015). "Long-Term Formaldehyde Emissions from Medium-Density Fiberboard in a Full-Scale Experimental Room: Emission Characteristics and the Effects of Temperature and Humidity." Environ Sci Technol **49**(17): 10349-10356.

Ng, L., A. Persily and S. Emmerich (2015). Infiltration and Ventilation in a Very Tight, High Performance Home. 36th AIVC Conference Effective Ventilation in High Performance Buildings. Madrid, Spain, Air Infiltration and Ventilation Centre**:** 719-726.

OEHHA (2014). OEHHA Acute, 8-hour and Chronic Reference Exposure Level (REL)s, California Office of Environmental Health Hazard Assesement. from http://oehha.ca.gov/air/allrels.html.

Poppendieck, D. G., L. C. Ng, A. K. Persily and A. T. Hodgson (2015). "Long term air quality monitoring in a net-zero energy residence designed with low emitting interior products." Building and Environment **94**: 33-42.

Salthammer, T., S. Mentese and R. Marutzky (2010). "Formaldehyde in the Indoor Environment." Chemical Reviews **110**: 2536-2572.

Singer, B. C., B. K. Coleman, H. Destaillats, A. T. Hodgson, M. M. Lunden, C. J. Weschler and W. W. Nazaroff (2006). "Indoor secondary pollutants from cleaning product and air freshener use in the presence of ozone." Atmospheric Environment **40**(35): 6696-6710.

Waring, M. S., J. A. Siegel and R. L. Corsi (2008). "Ultrafine particle removal and generation by portable air cleaners." Atmospheric Environment **42**(20): 5003-5014.

Wei, W., C. Howard-Reed, A. Persily and Y. Zhang (2013). "Standard formaldehyde source for chamber testing of material emissions: model development, experimental evaluation, and impacts of environmental factors." Environ Sci Technol **47**(14): 7848-7854.

WHO (2010). WHO Guidelines for Indoor Air Quality: Selected Pollutants, World Health Organization. from http://www.euro.who.int/__data/assets/pdf_file/0009/128169/e94535.pdf.

Measuring Flame Retardant Emissions from Spray Polyurethane Foam in a Home

Dustin Poppendieck[1]
Angelica Connor[2]

[1]Engineering Laboratory, National Institute of Standards and Technology
100 Bureau Drive Gaithersburg, MD 20899
[2]Drexel University, Philadelphia PA

Content submitted to and published by:
Healthy Building 2015 Conference

U.S. Department of Commerce
Penny Pritzker, Secretary of Commerce

National Institute of Standards and Technology
Willie E May, Director

NIST National Institute of Standards and Technology • U.S. Department of Commerce

Poppendieck, Dustin; Connor, Angelica .
“Measuring Flame Retardant Emissions From Spray Polyurethane Foam in a Home.”
Paper presented at the Healthy Buildings 2015 Conference, Boulder, CO, Jul 19-Jul 22, 2015.

DISCLAIMERS

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Any link(s) to website(s) in this document have been provided because they may have information of interest to our readers. NIST does not necessarily endorse the views expressed or the facts presented on these sites. Further, NIST does not endorse any commercial products that may be advertised or available on these sites.

Poppendieck, Dustin; Connor, Angelica .
“Measuring Flame Retardant Emissions From Spray Polyurethane Foam in a Home.”
Paper presented at the Healthy Buildings 2015 Conference, Boulder, CO, Jul 19-Jul 22, 2015.

MEASURING FLAME RETARDANT EMISSIONS FROM SPRAY POLYURETHANE FOAM IN A HOME

Dustin POPPENDIECK[1,*] Angelica CONNOR[1,2]

[1]Indoor Air Quality and Ventilation Group, Engineering Laboratory, 100 Bureau Drive, Mail Stop 8633, Gaithersburg, MD 20899-8633

[2]Currently at Drexel University, 3141 Chestnut Street, Philadelphia, PA 19104

[*]Corresponding email: dustin.poppendieck@nist.gov

Keywords: Spray polyurethane foam, emissions, TCPP

SUMMARY

The use of spray polyurethane foam (SPF) insulation in the United States is increasing. The primary flame retardant used in SPF, Tris (1-chloro-2-propyl) phosphate (TCPP), has been detected in micro-chamber emission experiments investigating SPF. However, due to the use of TCPP in furniture, SPF has not previously been positively identified as a source of indoor TCPP concentrations. This research measured airborne TCPP concentrations in a furniture-free residential test facility that contained 15 m^2 of exposed, two-year-old, open cell SPF.

INTRODUCTION

Spray polyurethane foam (SPF) insulation is increasingly being used in both new construction and retrofits. SPF is a unique building product in two ways: 1) SPF reduces both convective and conductive heat loss through the building envelope, and 2) SPF is created on site through the reaction of two sets of chemicals. Chemicals used to make SPF include polyols, isocyanates, amines, surfactants, amine polyols, alkanolamines, blowing agents and flame retardants. SPF can contain more than 8 % flame retardant (Sebroski 2012). Recent research (Poppendieck et. al. 2015) has shown than when a sample of new open cell, high pressure SPF was tested in micro-chamber environments at 40 °C and 100 mL/min, the flame retardant Tris (1-chloro-2-propyl) phosphate (TCPP) was emitted at nearly a constant concentration (400 μg/m^3 to 500 μg/m^3). However, it is unclear how TCPP emissions emission factors from SPF micro-chamber experiments relate to TCPP sources and concentrations in buildings. TCPP is also used in products that contain polyurethane foam such as furniture, mattresses and sound insulation within consumer products. Hence, if TCPP is measured in air of an occupied house containing SPF, the TCPP source cannot be solely attributed to the insulation or the furniture.

The National Institute of Standards and Technology (NIST) built in 2012 a net-zero energy residential test facility (NZERTF) to support the development and adoption of cost-effective net-zero energy designs and technologies, construction methods, and building codes. The design and construction of the NZERTF are described in Pettit et al. (2014). The NZERTF is a two-story, detached home with an unfinished basement and attic within the building thermal envelope. The garage is not attached. The house is similar in size (242 m^2 for occupied floors, 485 m^2 inside the building envelope including the attic and basement) and aesthetics to homes in the surrounding communities. To achieve the net-zero energy goals, several technologies are employed, including a high efficiency heat pump, a solar hot water system, a heat recovery ventilator (HRV), and a 10.2 kW photovoltaic system. To comply with the outdoor air requirements in ASHRAE Standard 62.2-2010 (2010) the HRV was sized to deliver 137 m^3 h^{-1} of outdoor air. Special attention was paid to the design and construction of the highly insulated and airtight building envelope. Roughly 15 m^2 of high pressure, open cell SPF was used to insulate the basement rim joists. The basement is unfinished and the SPF is not covered by any finishing material. The house has no carpet and is not furnished other than permanently installed cabinetry. Hence, if TCPP is present in the indoor air of the house and not measured in the outdoor air it can likely be attributed to the SPF. This work sought to measure airborne TCPP concentrations in the NZERTF.

METHODOLOGIES

The first floor and basement of the NZERTF were sampled for TCPP over a period of two months. The NZERTF TCPP sampling involved two Tenax sorbent tubes in series. The first tube is used to quantify the TCPP concentration and the second to evaluate if there was breakthrough through the first. If TCPP breakthrough to the second tube was found, the data was not used. For each sampling event three sets of tubes were prepared.

Each tube set was sampled at 50 mL/min using a mass flow controller sampling system. Sampling times varied from 52 min to 216 min (average 155 min). The tubes were separated and spiked with internal standard (1.0 μL of 1.25 mg Toluene D-8/mL of methanol). Blank tubes (with internal standard) were run between the samples to quantify any carryover between samples. Samples were analyzed using a thermal desorption-gas chromatography/mass spectrometer system (TD-GC/MS).

When used in field applications TCPP typically consists of three isomers: tris(1-chloro-2-propyl) phosphate (≈66%), bis(1-chloro-2-propyl) (2-chloropropyl) phosphate (≈30%) and (1-chloro-2-propyl) bis(2-chloropropyl) phosphate (≈4%). The relative response ratios of the three isomers on the tubes with TCPP and the subsequent blanks were summed to determine the total response ratio. The combined relative response ratio was then integrated using a five point standard curve (20 ng, 30 ng, 50 ng, 70 ng and 90 ng). Typically, only the first two isomers were detected and only the first two isomers were quantified.

The 13 standard curve R-square values averaged 0.98 for the first and second isomer. On days when a standard curve was not run, check standards were run. The instrument detection limit was 8.65 ng and the method detection limit was 0.71 μg/m^3 to 2.86 μg/m^3 depending on the sample volume. Only values above the method detection limit for the corresponding sampling volume are shown below.

Samples were run over a period of two months in the summer of 2014. The initial thermostat set point (located on the first floor) was 23.9 °C, a setting that had been maintained for weeks prior to the analysis. The thermostat was raised to 32.2 °C and maintained at the temperature for a period of seven days. Temperatures in the basement were several degrees cooler than the thermostat set points. Temperature values shown in the following table and figure are 12-hour average readings from a thermocouple located in the center of the open basement.

To ensure that there we no sources of TCPP other than the SPF in the basement, small samples of a variety of materials with foam components were placed in a micro-chamber at 40 °C and sampled for TCPP using the same Tenax sorbent tubes and TD-GC/MS analysis. The sampled materials include rigid expanded polystyrene insulation, duct insulation, and two varieties of pipe insulation. No TCPP was detected from any of these materials (method detection limit 2.0 µg TCPP/g material m^3 air to 6.3 µg TCPP/g material m^3 air).

RESULTS AND DISCUSSION

Samples were taken in the basement and on the first floor with the HVAC (Heating, Ventilating, and Air Conditioning) operating under normal conditions (typical air change rates: 0.15 h^{-1} to 0.22 h^{-1}, Poppendieck et. al. 2015). Samples were also taken outdoors and no TCPP was detected. Table 1 shows that the average TCPP concentration for the basement samples was nearly twice that of the first floor samples. These data lends credence to the source of the TCPP being in the basement. As mentioned above, none of the other measured materials in the basement contained TCPP and there have never been other potential sources of TCPP, such as furniture or mattresses, in the NZERTF. This information indicates TCPP is being emitted from the SPF located in the basement, is transported to the living areas, and is measurable in the indoor air under normal operating conditions.

Table 1: Average TCPP concentrations measured in the NIST NZERTF.

Location	Average Temperature (°C)	Number of Samples (n)	Average Concentration (µg/m^3)	Relative Standard Deviation
1st Floor	23.7	9	1.5*	7.0%
Basement	21.0	12	2.8	9.9%

*First floor samples ranged from 13 ng to 16 ng per sorbent tube. This is below the lowest standard, but above the instrument detection limit of 8.65 ng determined according to “Definition and procedure for the determination of the method detection limit – Revision 1.11” Pt. 136, App. B 40 CFR Ch. I (7–1–03 Edition).

Direct comparisons of measured concentrations (Table 1) to other residences is of limited use given the unique conditions of the NZERTF. First, SPF was not the primary insulation used in the house. SPF was only sprayed on 15 m^2 of the house exterior, a relatively small fraction of the greater than 600 m^2 of the building envelope. Other SPF application scenarios may involve a larger fraction of the building envelope. Second, the SPF was directly exposed to the basement air. In many SPF applications there are finishing products between the SPF and the occupied space. These products, such as drywall, can inhibit the transfer of TCPP to the occupied space. Third, there were no other sources of TCPP (furniture and mattresses) present in the house. Fourth, this work did not quantify the sorption and or re-emission of TCPP from dust or any other materials. Finally, the toxicological relevance of these concentrations is beyond the scope of this paper. There is limited data on chronic exposure to low TCPP concentrations (Farhat et. al. 2013). Current efforts to expand this knowledge are underway by other researchers.

Previous work (Poppendieck et. al. 2015) has shown a strong correlation between TCPP concentration and temperature when sampled in controlled micro-chamber experiments. To see if this relationship also held true in a full scale residence, the temperature of the NZERTF was raised for seven days (average basement temperate 28.5 °C). The results in Figure 1 illustrate the TCPP concentrations in the NZERTF are also strongly correlated to indoor temperature. There was minimal correlation with outdoor temperature (R square 0.03). The average outdoor temperature was 23 °C during both sets of indoor temperature experiments.

These data are consistent with the micro chamber data that demonstrate a relationship between temperature and emission rate of TCPP from SPF insulation. More research is needed to determine building envelope temperatures where SPF is applied and the fate and transport of TCPP through wall finishing materials.

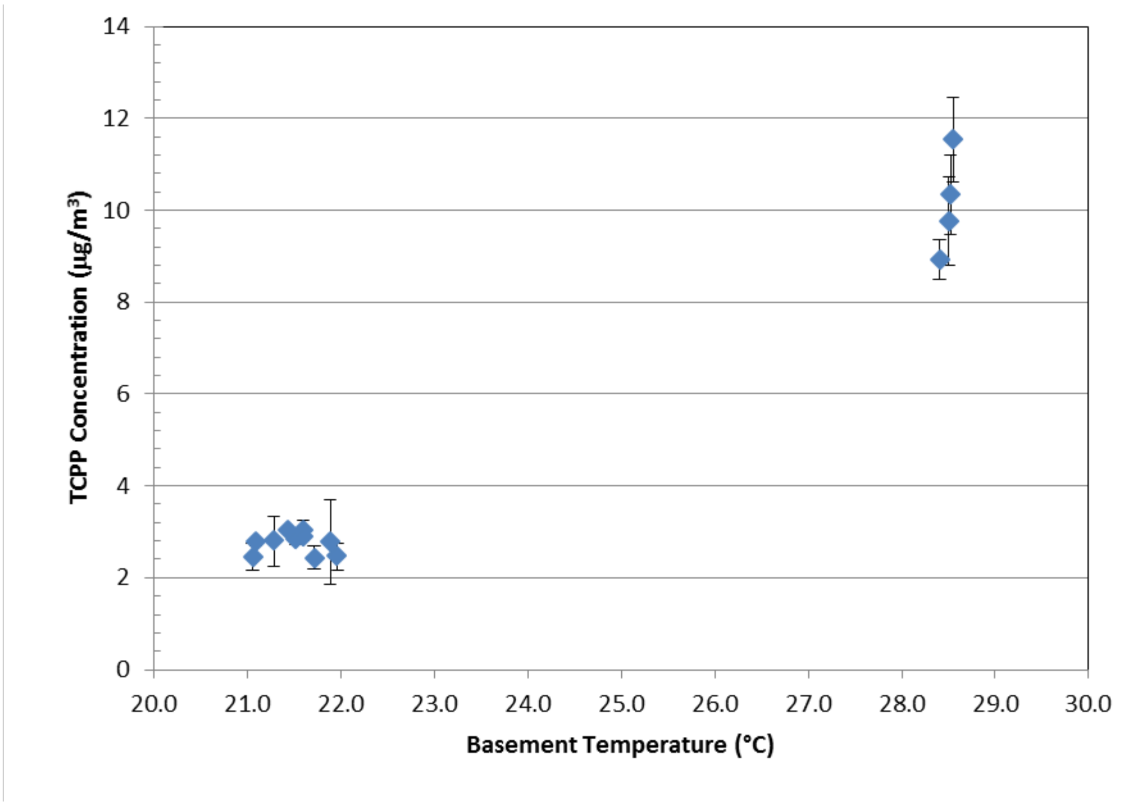


Figure 2: TCPP concentrations measured in the NIST NZERTF basement at various temperatures. Error bars show two standard deviations of triplicate sampling.

CONCLUSIONS

This research indicates that under the tested conditions, airborne TCPP concentrations can be measured in the NZERTF and the source of the TCPP is likely exposed, two-year-old, open-cell SPF.

REFERENCES

ASHRAE. Standard 62.2-2010: Ventilation and Acceptable Indoor Air Quality in Low-Rise Residential Buildings. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.; 2010.

Farhat, A.; Crump, D.; Chiu, S.; Williams, K. L.; Letcher, R. J.; Gauthier, L. T.; Kennedy, S. W. (2013). "In Ovo effects of two organophosphate flame retardants--TCPP and TDCPP--on pipping success, development, mRNA expression, and thyroid hormone levels in chicken embryos." Toxicol Sci 134(1): 92-102.

Pettit B, Gates C, Fanney AH, Healy W. Design Challenges of the NIST Net Zero Energy Residential Test Facility. TN-1847. Gaithersburg, MD: National Institute of Standards and Technology; 2014.

Poppendieck, D. Ng, L., Persily, A., Hodgson, A. Long Term Air Quality Monitoring in a Net-Zero Energy Residence Designed with Low Emitting Interior Products. Submitted Atmospheric and Environment. April 2015.

Poppendieck, D. Nabinger, S., Schlegel, M., Connor, A., Persily, A., Biggs, M., Thomas, T. Emissions from Open Cell Spray Polyurethane Foam Insulation. Submitted Building and Environment. May 2015.

Sebroski, J. Research Report for Measuring Emissions from Spray Polyurethane Foam (SPF) Insulation. Center for the Polyurethanes Industry (CPI) of the American Chemistry Council, September 4, 2012

Does Your SEM Really Tell the Truth?—How Would You Know?
Part 4: Charging and its Mitigation

Michael T. Postek[#] and András E. Vladár[#]
Semiconductor and Dimensional Metrology Division
[#]National Institute of Standards and Technology[1,2]
Gaithersburg, MD 20899 USA

ABSTRACT

This is the fourth part of a series of tutorial papers discussing various causes of measurement uncertainty in scanned particle beam instruments, and some of the solutions researched and developed at NIST and other research institutions. Scanned particle beam instruments, especially the scanning electron microscope (SEM), have gone through tremendous evolution to become indispensable tools for many and diverse scientific and industrial applications. These improvements have significantly enhanced their performance and made them far easier to operate. But, the ease of operation has also fostered operator complacency. In addition, the user-friendliness has reduced the apparent need for extensive operator training. Unfortunately, this has led to the idea that the SEM is just another expensive "digital camera" or another peripheral device connected to a computer and that all of the problems in obtaining good quality images and data have been solved. Hence, one using these instruments may be lulled into thinking that all of the potential pitfalls have been fully eliminated and believing that, everything one sees on the micrograph is always correct. But, as described in this and the earlier papers, this may not be the case. Care must always be taken when reliable quantitative data are being sought. The first paper in this series discussed some of the issues related to signal generation in the SEM, including instrument calibration, electron beam-sample interactions and the need for physics-based modeling to understand the actual image formation mechanisms to properly interpret SEM images. The second paper has discussed another major issue confronting the microscopist: specimen contamination and methods to eliminate it. The third paper discussed mechanical vibration and stage drift and some useful solutions to mitigate the problems caused by them, and here, in this the fourth contribution, the issues related to specimen "charging" and its mitigation are discussed relative to dimensional metrology.

Keywords: calibration, charging, measurements, metrology, modelling, scanning electron microscope, SEM, standards, reference materials

1.0 INTRODUCTION

Scanning electron microscopes are used extensively in research and advanced manufacturing for materials characterization, metrology and process control. Earlier papers [1 – 3], discussed some of the potential issues and pitfalls to avoid when quantitative measurements are made with an SEM. The first paper in the series discussed signal generation, instrument calibration, electron beam interactions, and the need for modeling to understand the mechanisms of the actual image generation [1]. Modeling has been discussed at greater length in other papers [4-5].

The second paper in the series, addressed another major issue confronting the microscopist, which is specimen contamination and methods of contamination reduction and its elimination [2]. In a third paper, the additional components of measurement uncertainty induced by mechanical vibration and stage drift and some possible solutions to these issues were discussed [3]. In this, the fourth contribution, some of the issues related to specimen "charging" and methods for its mitigation are discussed. All four of these tutorial papers are unified in the discussion of how these particular problems effect

[1] Contribution of the National Institute of Standards and Technology, not subject to copyright.

[2] Certain commercial equipment is identified in this report to adequately describe the experimental procedure. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the equipment identified is necessarily the best available for the purpose.

Scanning Microscopies 2015, edited by Michael T. Postek, Dale E. Newbury, S. Frank Platek, Tim K. Maugel,
Proc. of SPIE Vol. 9636, 963605 · © 2015 SPIE · CCC code: 0277-786X/15/$18 · doi: 10.1117/12.2195344

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

dimensional measurements made with the SEM. Over the years, several workers at NIST and other institutions have done a great deal of research into these issues in order to improve the fundamental metrology with particle beam instruments and some of this work, including some historical perspectives, is reviewed and discussed here.

2.0 DISCUSSION

2.1 Specimen Charging. The term "charging" in a particle beam instrument relates to the build-up of either positive or negative potential at or near the surface of a sample while it is being irradiated by a particle beam. Charging results in a significant number of undesirable consequences, and in a few cases, it can be used to the advantage of the researcher (see: Section 4.0). Surface charging causes instability of the secondary electron image intensity which results in variations in the secondary electron yield and detector efficiency. Changes in the surface potential also alters the primary beam landing energy resulting in changes in magnification, beam drift, image distortions and potential errors, even in x-ray microanalysis. All of the issues induced by charging are detrimental to measurement data quality.

Charging has been studied [6 - 9], but is not all that well understood. As discussed more extensively below, one can divide the possible cases of sample charging into four broad categories: **non-charging** - this is the case of metals, i.e., conductive samples where the primary beam electrons can readily travel to ground potential; **un-noticeable charging -** charge build-up is sufficiently minor that the operator does not readily observe obvious charging-related problems during the imaging and measurements of partially conductive, grounded samples. This is the most troublesome case since it often not recognized until after the micrograph has been taken; **evidently charging -** partially conductive samples that still allow limited imaging and measurements; and **grossly charging -** non-conductive and or non-grounded samples that preclude any meaningful imaging or measurements.

Maxwell's equations dictate that charge must be conserved, this is an accounting relationship. When viewing an ideal conductive sample at high accelerating voltage, the sum of the backscatteded electrons leaving the sample (backscattered electron coefficient - η), the secondary electrons leaving the sample (secondary electron coefficient - δ) as signal, may be less than unity but, must be balanced by those electrons flowing to ground, this can be measured as the specimen current. In an ideal case, the specimen current measured (I_{sc}) is a function of the beam energy (E). If incident beam current is represented as (I_{beam}) then:

$$-I_{beam} + (\eta+\delta)I_{beam} + I_{sc} = 0$$

and for a conductive sample, that is typically, the case. Therefore, when ($\eta+\delta$) is unity the measured I_{sc} is zero.

Unfortunately, most of the more interesting samples are not ideal. In most cases, there are differences in the current flow to earth between the I_{beam} and the I_{sc} . Those difference relate to the conductivity, the total signal leaving the sample and how much charge remains:

$$I_{sc} = 1 - (\eta+\delta).$$

In a non-conductor, I_{sc} = O, so charge can accumulate. If $\eta+\delta < 1$, negative charging will occur, and if $\eta+\delta > 1$, positive charging will result. In those cases where charge accumulates, the goal is to achieve a ***Dynamic Charge Balance*** so that: $\eta+\delta = 1$, so the number of electrons injected into the sample by the primary electron beam are balanced by those leaving the sample as signal [8]. Approaches to achieving that balance are discussed in Section 3.1 and Joy and Joy, 1996 [8].

The consequences of charge build-up in an SEM have been known and researched since the early days of television. This is because the early television and the SEM are both closely related technologically in that they were both scanned electron beam systems. Especially notable was the work at RCA Laboratories [10 - 12]. Aspects of that research were directly applicable to the early SEM instruments such as the ones developed by Zworykin, Hillier and Snyder [13] and those at Cambridge University [14 – 15] that ultimately led to the first commercial SEM instruments.

In some ways, charging is very capricious in that one can easily make a sample charge-up grossly (as discussed below), or subtle charging can go on essentially unnoticed and potentially result in significant measurement errors. This capricious

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

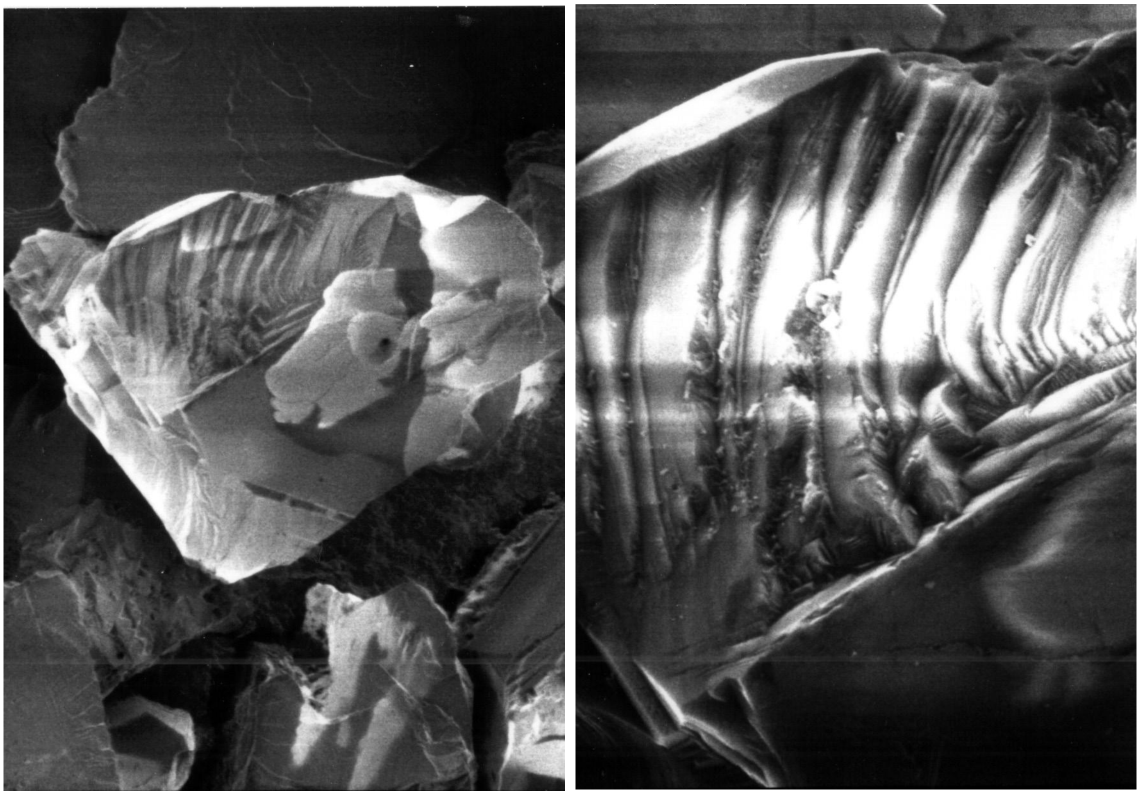


Figure 1. *Examples of negative charging of a diamond chip. (Left) Micrograph demonstrating minimal charging with low landing energy[3] at 1.0 keV (HFW[4] = 36 μm). (Right) Micrograph showing evidence of strong charging when the landing energy is increased to 10 keV, (HFV = 13 μm).*

nature is largely due to the dynamic nature of charging, to the versatility of the scanning electron microscope, and to the variety of geometries and instrument conditions available in the various particle beam instruments. Often a sample that is charging in one instrument may show no obvious sign of charging in another. There are many reasons why this is the case (as discussed below). In the past, most of the research work has revolved around finding ways to avoid charging. This is quite understandable since this is a rather complicated problem to solve because of the large number of possible instrument and sample variables. It is clear that it is up to the operator to recognize a charging situation and determine the proper conditions necessary to mitigate it and acquire the best images and measurement data.

2.2 Types of Charging. Of the four general cases described above, strictly speaking, it comes down to two types of specimen conditions that can be readily identified. These are non-charging and charging in the particle beam instrument.

2.2.1 Non-Charging. A highly conductive sample, such as bulk gold, channels all of the electrons that it absorbs to ground and no charging (i.e., change in electrical potential) would come about either during image acquisition or after. Clearly, that

[3] Low landing energy is used here since that term has replaced the term low accelerating voltage because in some of the newer instruments the electron source can emit electrons at high accelerating voltage, but they are decelerated to a lower landing energy in the column and/or at the sample stage. This technique allows the electron optical column to operate more optimally (See: Reference 1). In SEM literature, landing energy is usually given in kilo-electron volts (keV). For example, 15 kV accelerating voltage with no deceleration results in (approximately) a15 keV energy primary electron beam.

[4] Although, horizontal field width and field of view are often used interchangeably (See: Reference 1), HFW has been adopted in this publication since field of view implies a two - dimensional array which is only valid when the beam scan is normal to the sample (zero degrees of tilt).

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

is the most ideal situation. Most of the more interesting sample materials are not so cooperative. Even some, seemingly completely conductive metal samples, such as aluminum can have an oxide layer on the surface, can develop a charge depending upon the instrument conditions applied.

2.2.2 Charging. When a material cannot effectively conduct the beam energy imparted to it by the primary electron beam to ground it is often said to be "charging." This build-up of (or a change in) the electrical potential in or around the sample itself can result in detrimental effects to the imaging and any measurements made with the instrument on that sample. Samples may develop a static charge that - depending on the conductivity of the sample and its environment – can be retained for long periods of time, in vacuum. Generally, it is advantageous to allow the static charge to completely drain from the sample, because the changes induced by the primary electron beam of the instrument can be interpreted better and are more repeatably. The accumulated charge in the sample material represents a potential energy, and when it is drained, the sample achieves a more neutralized, more stable, less energetic state. Electrical connections, including surface conduction due to humidity, all play a role in discharging the sample. Two major categories of charging can occur:

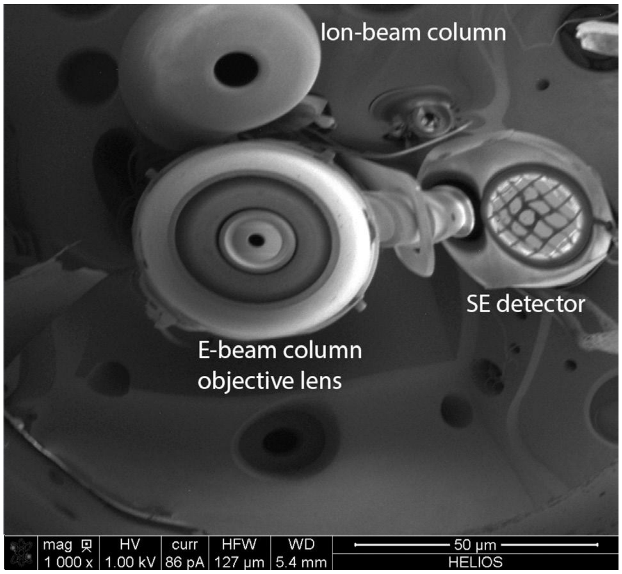


***Figure 2.** Example of extreme negative charging causing the primary electron beam to image the inside of the specimen chamber. The instrument "reports" it is scanning a horizontal field width (HFW) of 127 µm however, the stated magnification and HFV recorded on the micrograph are clearly wrong; the HFV is actually approximately 20 cm.*

2.2.2.1 Negative Charging - (η+δ < 1). Negative charge build-up occurs when a number of electrons impinging on the sample are trapped within the material and a negative electrical potential builds up. This can be only few volts or as much as the primary electron beam, i.e., several thousands of volts. The most common manifestation of this situation is that the image appears to "glow" (brighter) or cause geometry distortion in the image as electron production is artificially enhanced or the beam is unintentionally deflected (Figure 1). In other cases, marginally adhered particles can be seen to "blast-off" from the specimen stub – never to be seen again (until they land upon a critical component within the column). Fibers, insect antennae and other protruding structures will also be seen waving at the operator as the beam scans across them.

Since most samples are not totally conductive, charging is a common situation; a good deal of scientific literature has been devoted to this topic [16 – 18], as well as, the various references cited below. Negative charging is the most evident and troublesome type of charging and under the most extreme circumstances can disrupt and deflect the electron beam, and cause intolerable distortions. One of the first references to this, for the SEM, was Clarke and Stuart [19]. They formulated an explanation for the "formation of the distorted image of the electron collector of the scanning electron microscope when the instrument is used to observe uncoated insulating materials." This was provided as a cautionary note because they correctly felt it could lead to image misinterpretation when uncoated insulating materials were being observed.

Figure 2 shows an extreme case of charging resulting in a "mirror microscopy-like" image similar to the one described by Clarke and Stuart [19]. In this case, the sample has developed and is retaining a potential at or above that of the primary electron beam. The primary electron beam does not impinge on the sample, as it is scanned over the sample, but it is deflected throughout the specimen chamber generating signal from the internal components of the SEM specimen chamber, such as the final lens, and electron detectors [20, 21]. Even as strange as this mode of instrument operation is, it can also hold a diagnostic function since it can image particles and other contaminants on apertures and the final lens pole piece. Shaffner and Hearle, van Veld and Shaffner, and Shaffner and van Veld [22 - 24], reviewed the phenomenon of charging and also described the mirror mode described above and shown in Figure 2. The extreme negative charging at the sample, causes the primary electron beam to actually become diverted and image the inside of the specimen chamber. Images become grossly distorted and the primary electron beam is deflected as it approaches the sample throughout the chamber when such charging is present. Tilting the sample can direct the beam to various locations of interest. There does not ap-

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

pear to be any negative consequences to these actions, but it is startling to the operator the first time it occurs. This is an amusing application of charging, but this is not the main area where the typical charging problem exists. Typically the majority of problems exist between sample ground and just a few electron volts where subtle, un-recognized charging occurs.

Often, charging is obvious, but sometimes it is quite subtle. Negative charging presents an insidious problem for dimensional measurements because there is the potential for it to deflect the beam such that it actually lands nanometers away from its intended location. The amount of deflection can be negligible or it can be significant depending upon the instrument conditions and the 3-dimensional structure being measured. As shown in Figure 3, when the beam approaches a charging structure, its trajectory can be altered and the landing point where the signal is being generated and the point where the instrument scanning system believes the landing point can be different, hence leading to erroneous data and measurements. The delta (Δ) of this measurement is exaggerated for effect, and the amount of deflection is variable and depends on the electrical potential, the structure of charging sample, and on the landing energy[3] of the electron beam. This effect was postulated by Postek [21] for photomask metrology and was later demonstrated by Davidson and Sullivan [22] who calculated the electric fields on dielectric materials and showed, with modeling and experimentation that measurements in the SEM could be compromised by several nanometers if charging of only a few volts was occurring on the sample. Further work in this area needs to be done in order to fully understand the uncertainty that such charging poses to the accuracy of any measurement. However, it is very important to be aware of the potential uncertainty this introduces into the measurement process and to work to eliminate charging in all possible cases.

2.2.2.2 Positive Charging - (η+δ > 1). Positive potential can build up when more electrons are emitted from the sample than the primary electron beam provides. The positively charged regions rather than glowing brighter, get darker, because the secondary electron (SE) emission is reduced, many of the SEs are attracted back to the sample surface. Positive charging turns the scanned area dark and it is often confused with the build-up of contamination (which was discussed in Reference 2). Positive charging is far less detrimental than negative charging, and it is usually restricted only to a few volts of electrical potential. The main result is a loss of some valuable signal electrons as they are re-absorbed by the positively charging surface [27, 28]. Figure 4 shows an interesting effect of the deposition of positive charging on a thin oxide film sample. The initial "writing" of the dark lines was carried out by the automatic exposure (contrast, brightness) setting circuitry that was scanning only over the partial field, resulting in the widely spaced dark scan lines. The acquisition of the final overall image was then taken with that exposure setting.

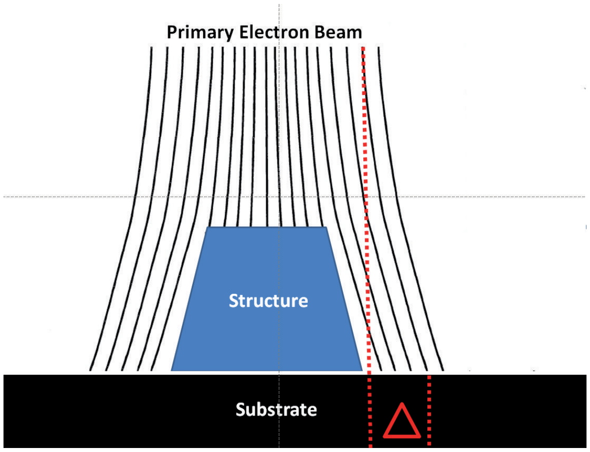


Figure 3. *Artistic representation of potential beam deflection due to charging. Charging of structures can result in the potential of beam deflection of several nanometers (re-drawn from Davidson and Sullivan [26]). The magnitude of the deflection (Δ) is a function of a number of factors as discussed in the text.*

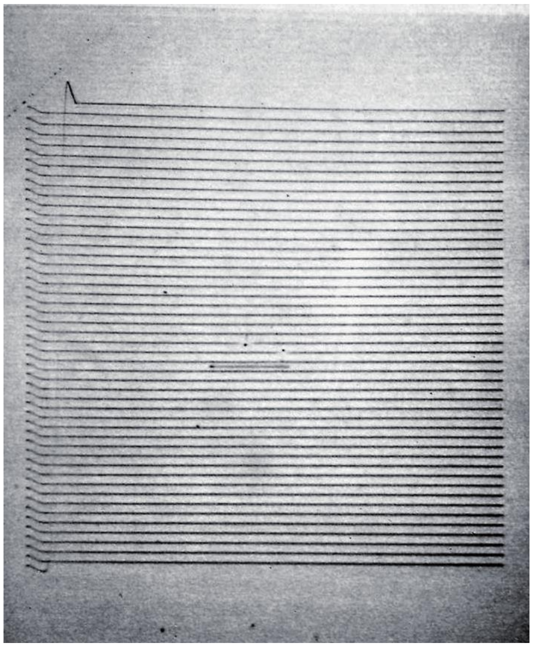


Figure 4. *Positive charging on a thin oxide film sample showing dark lines where the primary electron beam was scanned over the sample during the automatic exposure setting routine. In the case shown, the partial field scanning for the automatic exposure (contrast and brightness) adjustment resulted in positive charging on the portion of the sample exposed by the beam. After the initial adjustment, the final overall image was taken. Note the scan initiation, over-scanning and retrace can be clearly seen. The micrograph was taken at 1.0 keV (HFW = 2 250* μ*m).*

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

If that sample was allowed to remain in the instrument for a period of time, or removed and put back into the instrument, the dark lines will have disappeared since the charge dissipated due to the venting of the chamber.

2.2.3 Diagnosing Charging. Positive and negative charging can be diagnosed quite easily to determine the proper landing energy and the sample's conductivity, a further discussion can be found in Joy and Joy [9]:

- Set-up the instrument to the proper instrument operating conditions.
- Locate an area of interest and focus on that area at a high magnification or the magnification where one you plan to do the majority of the work (the effect of charging is exacerbated at higher magnifications).
- Irradiate the sample for a few seconds within the area selected.
- Reduce the magnification by a factor of 5 and observe the sample.
- If a bright raster pattern appears (which may slowly disappear upon going to the lower magnification), negative charging is probable. Therefore, try lowering the landing energy a few 100 eV. Then, repeat the procedure at a different location.
- If a dark raster pattern appears, and then (possibly) quickly disappears, positive charging is probable (Figure 3). If that occurs, raise the landing energy a few hundred volts. Then repeat the procedure.
- If the dark square remains, then positive charging is not likely to be the problem. Beam induced contamination is more likely the problem (see: Reference 2).

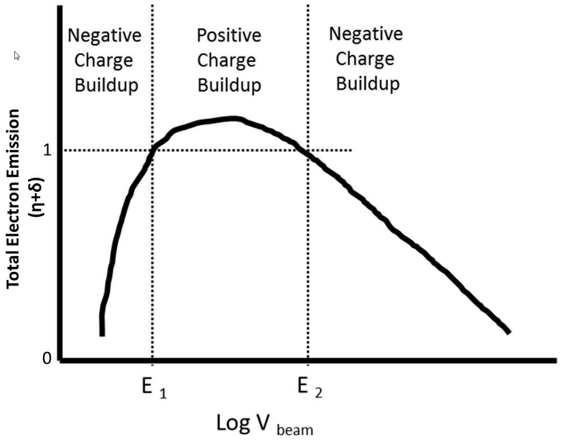


Figure 5. *Total electron emission curve. The E_1 and E_2 points are the landing energies where Dynamic Charge Balance is achieved and no sample charging is expected to occur.*

3.0 SOME METHODS FOR CHARGE MITIGATION

Studies of the phenomenon of sample charging were carried out since early work with the SEM. The SEMs relative similarity to early cathode-ray tube and television research led to many useful and parallel conclusions. The two most common approaches to the mitigation of charging are low accelerating voltage (low landing energy) operation and coating the sample with a thin conductive metal or carbon layer. Other possible solutions are discussed later in Section 3.3.

3.1 Low Accelerating Voltage Observation. Low accelerating voltage (landing energy) operation was possible with most SEMs since the early days, but the imaging was generally poor due to instrument design, poor signal-to-noise ratio and lower resolution [29, 30]. It was not until the latter 1980s when scanning electron microscopes were able to routinely view most samples in a non-destructive, uncoated manner. Many innovative instrument improvements took place which eventually changed instrument operation and the terminology used to low landing energy techniques.[3] The notable improvements that spurred this was the availability of high brightness electron sources such as lanthanum hexaboride and field emission electron sources and later frame storage electronics which evolved into the current digital imaging electronics. Non-destructive, low landing energy operation became common in semiconductor manufacturing where insulating samples (such as oxides and photoresist) are viewed routinely on the production lines. Early research work in cathode ray tubes and television found that generally, at low landing energies, a charge balance could be achieved when an electron beam impinges on an insulating surface. Thornley [31] reported that at low (1-2 keV) landing energies the secondary electron coefficient could be greater than unity, as shown on Figure 5.

For most non-conductive materials, E_1 and E_2 are the points where the total electron emission is equal to 1. Joy and Joy have published data on a number of E_2 points [9]. It is thought that the E_1 and E_2 points are relatively stable for a particular sample and set of instrument conditions being applied (landing energy, beam current, tilt, etc.) and they are the energies at which the sample is in charge balance. At that point, the number of electrons injected into the sample by the primary

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

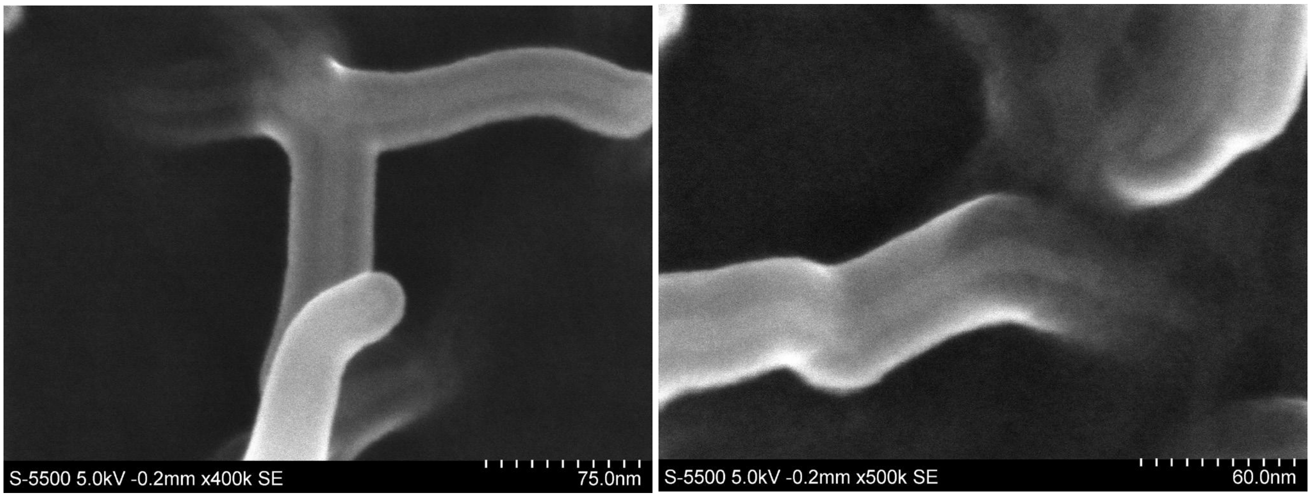


Figure 6. *Micrographs of cellulose nanofibrils that have been coated with osmium vapor in order to reduce the charging. The 6-7 nanometer visible core is likely the cellulose and the remaining thickness is the osmium vapor coating. Images taken at a landing energy of 5 keV (HFV, left = 250 nm, HFV, right = 316 nm).*

electron beam is equal to the total of those electrons leaving the sample and thus no specimen charging presumably occurs. Usually there is a small range of voltages to which a sample can be exposed, up to and including the E_2 value. E_2 is the most stable value and is usually chosen for uncoated observation since it is found at a higher accelerating voltage, thus enabling a higher resolution operating condition for the instrument. However, the optimal landing energy needed is always dependent on the required sample information. A high voltage primary beam will image layers deeper into the sample, while low voltages will provide more information from the sample surface. So compromises must always be optimized. Additionally, newer particle beam instruments with ultra-low voltage/high resolution capability can work acceptably in the E_1 region without significant compromise to the resolution.

3.2 Specimen Coating. Traditionally, over-coating the non-conducting specimen with a heavy metal, conductive, material (gold, gold/palladium, and osmium) has been the most commonly used method to overcome charging. Coating also increases the secondary electron emission from the sample especially if the sample is composed of low atomic number materials (especially biological). The one thing that must be remembered is that, if a sample is coated, signal is mainly being generated from the flux of electrons originating from the coating acting as a protective shell and not necessarily the sample of interest. In addition, a myriad of coating artifacts, such as cracking, can result. Adding the appropriate amount of coating has always been a complicated decision based upon the needed conductivity and the amount of artifacts one can tolerate. Vacuum evaporation (gold, gold/palladium), sputter coating (gold, gold/palladium) and aqueous or vapor deposition of osmium have all been used. The philosophy and techniques can be found in Postek et al., [32]. For x-ray microanalysis often carbon coating is also helpful in reducing charging and diminishes the effects of stray artifacts in the analysis [33].

A good continuous coating can mitigate charging, but can also introduce coating artifacts such as a change in surface details. Coating also increases the size of the structures being observed relative to the thickness of the coating applied. Therefore, interpretations can be compromised. Figure 6 shows a nanocellulose material that has been coated with a deposition of a few nanometers of osmium vapor. Note that the core (observed through the coating) is about the expected 6-7 nanometers in diameter for the cellulose nanomaterial but, surrounding it is several additional nanometers of coating. Therefore, coating a nanoparticle potentially compromises the measurements especially on nano-sized particles and structures.

3.3 Other Potential Solutions. The simplest approach is often the best approach. Hence today, non-destructive low accelerating voltage operation is the first method usually applied to an unknown sample, then coating may be tried if needed. Seasoned microscopists usually begin by applying low landing energies to an unknown sample, unless they know coating will not compromise the imaging or measurements. However, as discussed below, other methods have also been used with varying degrees of success.

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

3.3.1 Charge Neutralization. Prior to the availability of high resolution imaging at low landing energies, Crawford [34, 35] and others reported good success with specimen charge neutralization. In this case, the charge build-up is neutralized, as it builds up, by a beam of very low energy ions. The ions act to stabilize the surface potential, at the "ion zero kinetic-energy point, independent of the nature of the insulating surface." [34] This requires the installation and optimization of a charge neutralization device in proximity to the sample. The unit is positioned above the specimen and below the final lens in the specimen chamber of the SEM. Because of the amount of specimen chamber real estate needed by the device and the prevalence of low landing energy microscopy with high-brightness field-emission instruments, this method is not often practiced, today. In the scanning helium ion microscopes there is an option for an electron flood gun to work to neutralize the positive charging caused by the ions.

3.3.2 Fast, TV-Rate Imaging. Welter and McKee (1972) [36] demonstrated that fast scanning using a high-brightness field-emission electron microscope could alleviate charging problems. They stated that "if a layer of charge is put down on the specimen and reinforced at a scan rate faster than the average discharge rate," charge equilibrium could be reached. They used a fixed TV scan rate of 1155 lines per frame and 15 frames/sec. and provided reasonable imaging even at low landing energies. This work paved the road for the more modern instruments displaying 60 frames/sec. (or greater). TV-rate imaging is now common on most instruments. But, it took successful demonstration of the concept of fast scanning with good signal-to-noise ratio to prove that charging could be mitigated in this manner.

3.3.3 Backscattered Electron Imaging. One of the earliest approaches to charge mitigation in the SEM was to employ backscattered electron collection rather than secondary electron collection. Charging of the sample affects the secondary electron image far more than the higher-energy backscattered electrons. Most laboratory SEMs are equipped with a mechanism whereby the bias of the collection screen at the front of the SE detector can be grounded or negatively (reverse) biased, thus rejecting the SE and only allowing those high-energy BSEs that are in the proper geometrical relationship to the detector to be collected. Alternatively, dedicated backscattered electron detectors can be employed. Tilting the sample toward the detector is, not only, helpful to improve signal collection but alsom signal strength. BSE detection is also used on uncoated samples in the table-top instruments. Alternatively, the low loss technique developed by Wells [37] was shown to provide high-resolution images of the sample surface while mitigating the charging.

3.3.3.1 Low-Loss Electron Imaging. Low loss imaging is a subset of backscattered electron imaging where the electrons are energy filtered in such a manner that only those that have minimally interacted with the sample are collected. These are the low loss electrons. These electrons have been demonstrated to have greater surface sensitivity and reduced apparent charging [38 – 41]. Overall, sample charging is not eliminated and beam deflection by surface charging can still occur - the charging is not dissipated, just ignored. If the charge builds up sufficiently, deflection of the primary electron beam is still possible.

3.3.4 Conductive Spray. Prior to the prevailing use of high-resolution low landing energy microscopy, experiments were undertaken to use a "conductive" spray to eliminate charging. As early as 1957, Wells [15] described experiments with several potential anti-static materials. It is notable that, conductive spray was reported to be successfully used on polymers by Sikorski et al. (1967) [42] to view polymers with no or reduced charging at high landing energies. A "conductive film aerosol" was marketed in 1980, as a commercial product, but was taken off the market several years later. A similar product has been recently revived as ConductCoat [43]. This product appears to have some success in reducing charging on some materials, but an overall comparison if this material to low landing energy operation has not been done, nor have the effects on instrument or specimen contamination been fully studied.

3.3.5 Variable Pressure SEM. It is clear that, charging must be overcome in order to obtain any meaningful data from the SEM. Gross charging can readily distort the image and subtle charging can deflect the beam and lead to measurement error. An alternative that has not been fully explored for metrology is the employment of variable pressure or "environmental" microscopy [44 - 47]. This methodology uses a gaseous environment to neutralize the charge. For various technical reasons, high-pressure microscopy has mostly been employed for specimens of a biological nature, not for many semiconductor samples. Figure 7 shows several images of photomask samples taken at high landing energies usingt variable pressure technoloogy demonstrating no charge accumulation. Photomasks are very prone to charging [48]. It has been reported that high accelerating voltage, injection of air of as little as 20 Pa ~0.15 Torr into the specimen chamber can reduce the charging

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

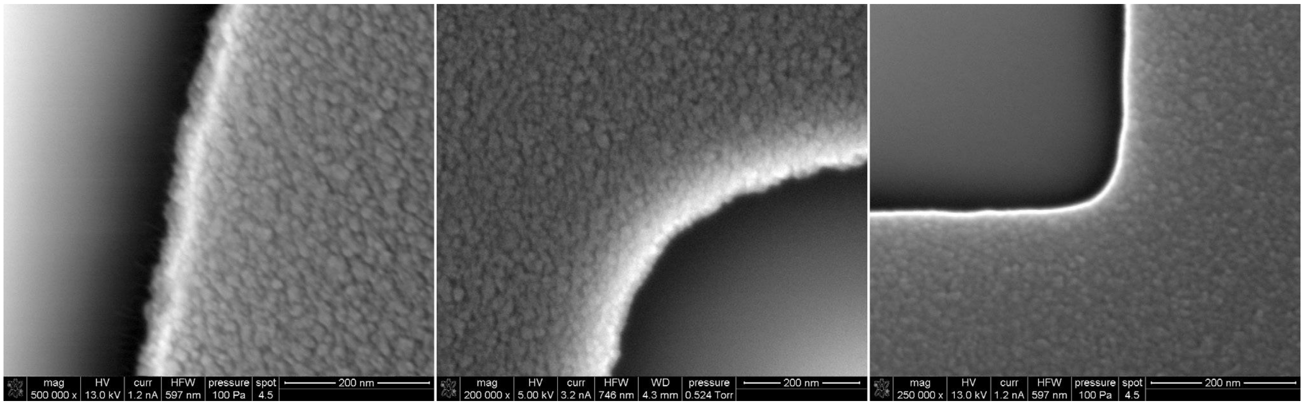


Figure 7. *SEM Micrographs of several chromium photomask samples using the variable pressure SEM. (Left) 13 keV landing energy (HFW =597 nm); (Center) 5keV landing energy (HFW = 746 nm); (Right) 13 keV landing energy (HFW =597 nm).*

potential of an insulator at the surface by as much as an order of magnitude [49]. For accurate metrology, this methodology affords a path that minimizes, if not eliminates, the need for charge modeling. Modeling of charging is exceptionally difficult since each sample, instrument and operating mode can respond to charging in different ways. This methodology shows great potential if optimal balance can be achieved in a reproducible manner. This methodology, although potentially desirable for charge neutralization, has not been seriously employed in photomask or wafer metrology [50]. This is largely because there is not an instrument available for full-scale production samples with high throughput. VPSEM was proven to be useful for photomask metrology [51] but no in-line instrument was developed to use the technology, either. Variable pressure microscopy offers advantages of possible application of higher accelerating voltages and different contrast mechanisms [51].

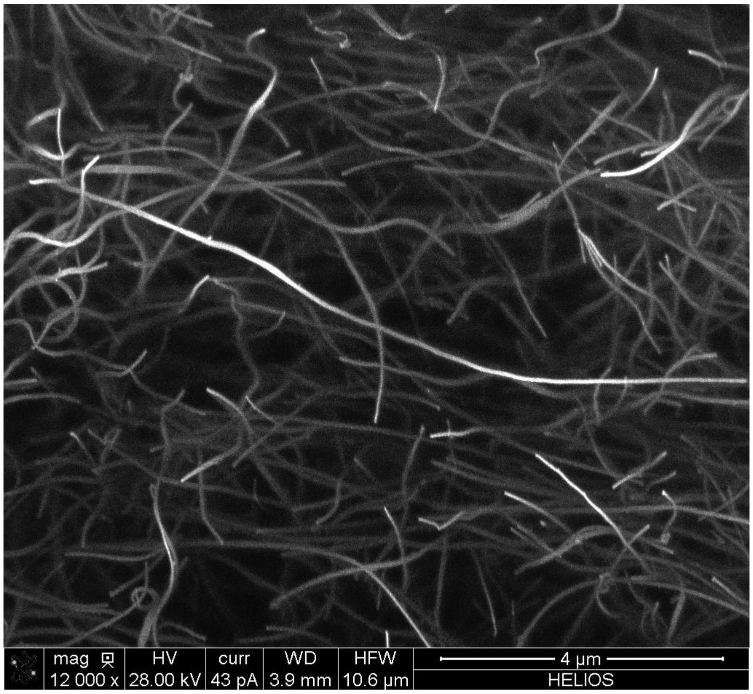


Figure 8. *Micrograph of tangled multiwall CNT structures in an epoxy matrix taken at 28keV (HFW = 10.6 µm) those that are sharper reside close to the surface and others are several nanometers below the surface (See: Reference 55).*

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

4.0 ADVANTAGES AFFORDED BY SAMPLE "CHARGING"

On the other side of the coin, charging can be used and advantageously controlled. Charge contrast forms the basis of several imaging modes such as voltage contrast (VC) and electron beam induced conductivity (EBIC). Both of these methods are used extensively in semiconductor electronics testing and quality control [27, 52, and 53].

4.1 Charge Contrast. More recently, some conductive materials buried on non-conducting matrices have been shown to be successfully imaged using charge induced contrast (Figure 8). By properly choosing the instrument operating conditions, sub-surface imaging of materials, such as carbon nanotubes (CNT) in polymers (epoxy) can be imaged even embedded as deeply as several hundred nanometers [54, 55].

5.0 CONCLUSION

Charging is an inevitable consequence of particle beam microscopy of non-conductive samples. It is clear that charging must be overcome in order to obtain meaningful and repeatable data from the SEM. Coating of the sample to make it conductive is only one solution, which could lead to artifacts. Gross charging readily distorts the image and subtle charging can deflect the beam and hence can lead to measurement error. Charging can be overcome with judicious application of the methods discussed in this presentation. For general imaging, charging can be useful and it may create interesting micrographs, but for measurements it can lead to a great deal of error if the operator is not careful.

6.0 REFERENCES

[1] Postek, M. T., Vladár, A. E., "Does Your SEM Really Tell the Truth? How would you know? Part 1," SCANNING 35:355-361 (2013).

[2] Postek, M. T., Vladár, A. E., Kavuri, P. P., "Does Your SEM Really Tell the Truth? How would you know? Part 2. Specimen Contamination," SCANNING 36:347-355 (2014).

[3] Postek, M. T., Vladár, A. E., and Cizmar, P., "Nanomanufacturing Concerns about Measurements made in the SEM Part III: Vibration and Drift," SPIE 9173 917306 pp. 1 to 10 (2014).

[4] Postek, M. T., Vladár, A., "Modeling for Accurate Dimensional Scanning Electron Microscope Metrology: Then and Now," SCANNING 33: 111-125 (2011).

[5] Postek, M. T., Vladár, A. E. Lowney, J., Larrabee, R. D. and Keery, W. J., "Two- Dimensional Simulation and Modeling in Scanning Electron Microscope Imaging and Metrology Research," SCANNING 24:179-185 (2002).

[6] Cazaux, 1986, "Some Considerations on the Electric Field Induced in Insulators by Electron Beam Bombardment" J. Appl. Phys. 59:1418-1430.

[7] Joy, D. C. 1989. "Control of Charging in Low Voltage SEM. Scanning 11:1-4

[8] Joy, D. C. and Joy, C. 1995. "Dynamic Charging in the Low Voltage SEM. " JMSA 1(3): 109- 112.

[9] Joy, D. C. and Joy, C. 1996. "Low Voltage Scanning Electron Microscopy" Micron 27:247-263.

[10] Rose, A. and Iams, H., "Television pickup tubes using low-velocity electron-beam scanning," Proc. I. R. E. 547- 555 (1939).

[11] Zworykin, V. K., Morton, G., and Malter, L., "The secondary emission multiplier – a new electronic device," Proc. Inst. Radio Eng. 24(3) 351- 375 (1936).

[12] Zworkyin, V. A. and Morton, G., "Television: The electronics of image transmission," John Wiley and Sons New York, 646 (1945).

[13] Zworykin, V. A. Hillier, J and Snyder R., "A scanning electron microscope," ASTM Bulletin 117:15-33 (1942).

[14] McMullan, D., "Investigations relating to the design of electron microscopes," Dissertation Univ. of Cambridge 202 pp. (1952).

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

[15] Wells, O. C., "The construction of a scanning electron microscope and its application to the study of fibres," Dissertation Univ. of Cambridge, 153pp (1957).

[16] Lau, K. M., Drouin, D., Lavallée, E., and Beauvais, J., "The Impact of Charging on Low-Energy Electron Beam Lithography," Microscopy and Microanalysis, 10, pp 804- 809 (2004).

[17] Anger, K., Lischke, B., and Sturm, M., "Material surfaces for electron-optical equipment," SCANNING 5:39-44 (1983).

[18] Reimer, L., Golla, U., Böngler, R., Kassens, M., Schindler, B., and Senkel, R., "Charging of bulk specimens, insulating layers and free-supporting films in scanning electron microscopy," Optik 92(1) 14-22 (1992).

[19] Clarke, D. R. and Stuart, P. R., "An anomalous contrast effect in the scanning electron microscope," J. Phys. E: Sci. Instrum. 3: 705-707, (1970).

[20] Alvarez, A, Bonetto, R. Guerin, D., and Peez, C., "Images of the inner parts of scanning electron microscopes," Electron Optics Reporter (Norelco) 31:1EM 39-43 (1984).

[21] Eckert, R., "Inspecting the SEM Chamber with a charged polystyrene mirror," SCANNING 14:73-75 (1992).

[22] Shaffner, T. J. and Hearle, J. W. S., "Recent advances in understanding specimen charging. Scanning Electron Microscopy/1976 (Part 1)," IITRI Chicago, IL 60616 61-70 (1976).

[23] Van Veld, R. D., and T. J. Shaffner, "Charging effects in scanning electron microscopy." Scanning Electron Microscopy/1971, 19-24 IITRI, Chicago, Il 60616 (1971)

[24] Shaffner T. J., and van Veld R. D., "Charging effects in the scanning electron microscope," J. Phys. E Scientific Instruments 4(9): 633-637 (1971).

[25] Postek, M. T., "Low Accelerating Voltage Inspection and Linewidth Measurement in the Scanning Electron Microscope," SEM/1984/III, SEM, Inc. 1065-1074 (1984).

[26] Davidson, M. and Sullivan, N, "An investigation of the effects of charging in SEM based CD metrology," Proc. SPIE 3050 226-252 (1997).

[27] Postek, M. T. and Joy, D. C., "Submicrometer Microelectronics Dimensional Metrology: Scanning Electron Microscopy," NBS Journal of Research 92 (3): 205-228 (1987).

[28] Postek, M. T., "Critical Issues in Scanning Electron Microscope Metrology," NIST J. Res. 99(5): 641-671 (1994).

[29] Blake, D. F., "Low voltage scanning electron microscopy." Test and Measurement. World, 6:62-75 (1986).

[30] Mullerova, I. and Lenc. M., "Some approaches to low-voltage scanning electron microscopy," Ultramicroscopy 41(4) 399-410 (1992).

[31] Thornley, R. F. M., "Recent developments in scanning electron microscopy," Proc. European Regional Conf. on Elect. Microscopy Delft, Vol. 1 (Nederland Verein Electronen) pp. 173-176 (1960).

[32] Postek, M.T., Howard, K.S., Johnson, A.J., and McMichael, K., "Scanning Electron Microscopy - A Student Handbook," Ladd Research Industries, 305 pp (1980).

[33] Bastin, G. F. and Heijigers, H., "Quantitative electron probe microanalysis of non-conducting specimens: science or art?" Microscopy & Microanalysis, 10: 733-738 (2004).

[34] Crawford, C. K., "Charge neutralization using very low energy ions" SEM/1979/II SEM Inc., AMF O'Hare, Il 60666, 31-46 (1979).

[35] Crawford, C. K., "Ion charge neutralization effects in scanning electron microscopes," SEM/1980/IV SEM Inc., AMF O'Hare, IL 60666, 11-25 (1980)

[36] Welter, L. M., and McKee, A. N., "Observations on uncoated, non-conducting or thermally sensitive specimens using a fast scanning field emission source SEM," SEM1972 IITRI Chicago, Ill 60616 161-168 (1972).

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

[37] Wells, O. C., “Low-loss Image for Scanning Electron Microscope,” Appl. Phys. Lett. 19(7): 232-235 (1971).

[38] Wells, O. C., “Low-loss Electron Images of Uncoated Photoresist in the Scanning Electron Microscope,” Appl. Phys. Lett. 49(13): 764-766 (1986).

[39] Wells, O. C., “Low-loss Electron Images of Uncoated Non-Conducting Samples in the Scanning Electron Microscope,” Microbeam Analysis/1987 (Geiss, R. H., ed.) San Francisco Press, San Francisco CA. 76-78 (1987).

[40] Wells, O. C. and Rishton, S. A. “Studies of Poorly Conducting Samples by the Low-Loss Electron Method in the Scanning Electron Microscope” Proc. 52nd. Annual Meeting MSA, Bailey, G. W. and Garratt-Reed, A. J., Eds. 1022-1023 (1994).

[41] Postek, M. T., Vladár, A. E., Wells, O. C., and Lowney, J. L., “Application of the low- loss scanning electron microscope SEM image to integrated circuit technology. Part 1. Applications to accurate dimension measurements,” Scanning 23(5): 298–304 (2001).

[42] Sikorski, J., Moss J. S., Newman P.H, and Buckley, T., “A new preparation technique for examination of polymers in the scanning electron microscope,” J. Phys. E 2(1):29-31 (1968).

[43] Burnett, B., “An electro-conductive organic coating for scanning electron microscopy” SPIE Vol. 9236 92360L – 1 - 9236 92360L-9 (2014).

[44] Danilatos, G., “Foundations of environmental scanning electron microscopy,” Adv. Electron. Electron Phys. 71, 109–250 (1988).

[45] Danilatos, G., “Introduction to the ESEM instrument,” Microscopy Res. Tech. 25, 354–361 (1993).

[46] Donald, A., “The use of environmental scanning electron microscopy for imaging of wet and insulating materials,” Nature Materials 2: 511-516 (2003).

[47] Thiel, B. and Toth, M. “Secondary electron contrast in low-vacuum environmental scanning electron microscopy of dielectrics,” J. Appl. Phys. 97 051101-1 – 051101-18 (2005).

[48] Postek, M. T. and Vladár A. E., “New application of variable pressure/environmental microscopy to semiconductor inspection and metrology,” SCANNING 26:11-17 (2004).

[49] Joy, D. C., “The future of e-beam metrology: Obstacles and opportunities,” Proc. SPIE 4689, 1–10. (2002).

[50] Postek, M. T, Vladár, A. E., and Bennett, M., “Photomask dimensional metrology in the scanning electron microscope, Part 1: has anything really changed?” JM3 3(2): 212- 223 (2004).

[51] Postek, M. T. and Vladár, A.E., “Critical dimension metrology in the scanning electron microscope,” in Handbook of Silicon Semiconductor Metrology, (edited by A. Diebold, Dekker, New York), Chap. 14, pp. 295–333 (2000).

[52] Feuerbaum, H. P., “Electron beam testing: methods and applications,” Scanning 5:14-24 (1983).

[53] Leamy, H., “Charge collection scanning electron microscopy” J. App. Phys. 53 (R51-R80) (1982).

[54] Finnie, P., Kaminska, K., Homm, Y., Austing, D., Lefebvre, J., “Charge contrast imaging of suspended nanotubes by scanning electron microscopy, Nanotechnology 19: 335202 (6pp) (2008).

[55] Zhao, M., Ming, B., Kim, J-W, Gibbon, L., Gu, X., Nguyen, T., Park, C., Lillehei, P., Villarrubia,,J., Vladár, A. E., and Liddle, J. A., “New insights into subsurface imaging of carbon nanotubes in polymer composites via scanning electron microscopy,” Nanotechnology 26: 085703 12pp (2015).

Downloaded From: http://proceedings.spiedigitallibrary.org/ on 01/28/2016 Terms of Use: http://spiedigitallibrary.org/ss/TermsOfUse.aspx

Nanomanufacturing Concerns about Measurements Made in the SEM Part IV: Charging and its Mitigation

Michael T. Postek[#] and András E. Vladár[#]
Semiconductor and Dimensional Metrology Division
[#]National Institute of Standards and Technology[1,2]
Gaithersburg, MD 20899 USA

ABSTRACT

This is the fourth part of a series of tutorial papers discussing various causes of measurement uncertainty in scanned particle beam instruments, and some of the solutions researched and developed at NIST and other research institutions. Scanned particle beam instruments especially the scanning electron microscope (SEM) have gone through tremendous evolution to become indispensable tools for many and diverse scientific and industrial applications. These improvements have significantly enhanced their performance and made them far easier to operate. But, the ease of operation has also fostered operator complacency. In addition, the user-friendliness has reduced the apparent need for extensive operator training. Unfortunately, this has led to the idea that the SEM is just another expensive "digital camera" or another peripheral device connected to a computer and that all of the problems in obtaining good quality images and data have been solved. Hence, one using these instruments may be lulled into thinking that all of the potential pitfalls have been fully eliminated and believing that, everything one sees on the micrograph is always correct. But, as described in this and the earlier papers, this may not be the case. Care must always be taken when reliable quantitative data are being sought. The first paper in this series discussed some of the issues related to signal generation in the SEM, including instrument calibration, electron beam-sample interactions and the need for physics-based modeling to understand the actual image formation mechanisms to properly interpret SEM images. The second paper has discussed another major issue confronting the microscopist: specimen contamination and methods to eliminate it. The third paper discussed mechanical vibration and stage drift and some useful solutions to mitigate the problems caused by them, and here, in this the fourth contribution, the issues related to specimen "charging" and its mitigation are discussed relative to dimensional metrology.

Keywords: calibration, charging, measurements, metrology, modelling, scanning electron microscope, SEM, standards, reference materials

1.0 INTRODUCTION

Scanning electron microscopes are used extensively in research and advanced manufacturing for materials characterization, metrology and process control. Earlier papers [1 – 3], discussed some of the potential issues and pitfalls to avoid when quantitative measurements are made with an SEM. The first paper in the series discussed signal generation, instrument calibration, electron beam interactions, and the need for modeling to understand the mechanisms of the actual image generation [1]. Modeling has been discussed at greater length in other papers [4-5].

The second paper in the series, addressed another major issue confronting the microscopist, which is specimen contamination and methods of contamination reduction and its elimination [2]. In a third paper, the additional components of

[1] Contribution of the National Institute of Standards and Technology, not subject to copyright.

[2] Certain commercial equipment is identified in this report to adequately describe the experimental procedure. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the equipment identified is necessarily the best available for the purpose.

Nanoengineering: Fabrication, Properties, Optics, and Devices XII, edited by
Eva M. Campo, Elizabeth A. Dobisz, Louay A. Eldada, Proc. of SPIE Vol. 9556,
95560Q · © 2015 SPIE · CCC code: 0277-786X/15/$18 · doi: 10.1117/12.2186997

measurement uncertainty induced by mechanical vibration and stage drift and some possible solutions to these issues were discussed [3]. In this, the fourth contribution, some of the issues related to specimen "charging" and methods for its mitigation are discussed. All four of these tutorial papers discuss how these particular problems effect dimensional measurements made with the SEM. Over the years, several workers at NIST and other institutions have done a great deal of research into these issues in order to improve the fundamental metrology with particle beam instruments and some of this work, including some historical perspectives, is reviewed and discussed here.

2.0 DISCUSSION

2.1 Specimen Charging. The term "charging" in a particle beam instrument relates to the build-up of either positive or negative potential at or near the surface of a sample while it is being irradiated by a particle beam. Charging results in a significant number of undesirable consequences, and in a few cases, it can be used to the advantage of the researcher (see: Section 4.0). The consequences of charge build-up in an SEM have been known and researched since the early days of television. This is because the early television and the SEM are both closely related in that they were both scanned electron beam systems. Especially notable was the work at RCA Laboratories [6-8]. Aspects of that research were directly applicable to the early SEM instruments such as the ones developed by Zworykin, Hillier and Snyder [9] and those at Cambridge University [10 – 11] that ultimately led to the first commercial SEM instruments.

Charging has been studied, but is not that well understood. As discussed more extensively below, one can divide the possible cases of sample charging into four broad categories: **non-charging** - this is the case of metals, i.e., conductive samples where the primary beam electrons can readily travel to ground potential; **un-noticeable charging -** charge build-up is sufficiently minor that the operator does not readily observe obvious charging-related problems during the imaging and measurements of partially conductive, grounded samples. This is the most troublesome case since it often not recognized intil after the micrograph has been taken; **evidently charging -** partially conductive samples that still allow limited imaging and measurements; and **grossly charging -** non-conductive and or non-grounded samples that preclude any meaningful imaging or measurements.

In some ways, charging is very capricious in that one can easily make a sample charge grossly (as discussed below), or subtle charging can go on essentially unnoticed and potentially result in significant measurement errors. The capricious nature is largely due to the dynamic nature of charging, to the versatility of the scanning electron microscope, and to the variety of geometries and instrument conditions available in the various particle beam instruments. Often a sample that is charging in one instrument may show no obvious sign of charging in another. There are many reasons why this is the case (as discussed below). In the past, most of the research work has revolved around finding ways to avoid charging. This is quite understandable since this is a rather complicated problem to solve because of the large number of possible instrument and sample variables. It is clear that it is up to the operator to recognize a charging situation and determine the proper conditions necessary to mitigate it and acquire the best images and measurement data.

2.2 Types of Charging. Of the four cases described above, strictly speaking, it comes down to two types of specimen conditions that can be readily identified. These are non-charging and charging in the particle beam instrument.

2.2.1 Non-Charging. A highly conductive sample, such as bulk gold, channels all electrons that it absorbs to ground and no charging (i.e., change in electrical potential) would come about either during image acquisition or after. Clearly, that is the most ideal situation. Most sample materials are not so cooperative. Even some, seemingly completely conductive metal samples, such as aluminum can have an oxide layer on the surface, can develop a charge depending upon the instrument conditions applied.

2.2.2 Charging. When a material cannot effectively conduct the beam energy imparted to it by the primary electron beam to ground it is often said to be "charging." This build-up of (or a change in) the electrical potential in or around the sample itself can result in detrimental effects to the imaging and any measurements made with the instrument on that sample. Samples may develop a static charge that - depending on the conductivity of the sample and its environment – can be retained for long periods of time, in vacuum. Generally, it is advantageous to allow the static charge to completely drain from the sample, because the changes induced by the primary electron beam of the instrument can be interpreted better and are more

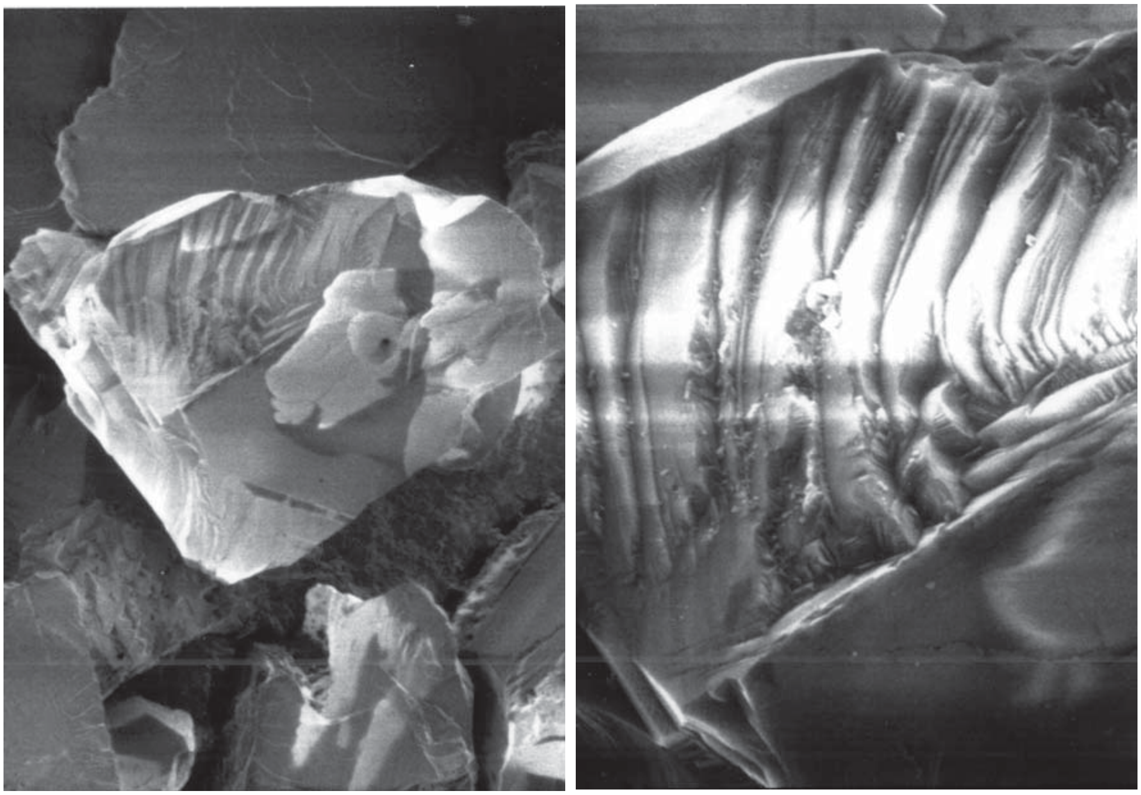


Figure 1. *Examples of negative charging of a diamond chip. (Left) Micrograph demonstrating minimal charging with low landing energy[3] at 1.0 keV (HFW[4] = 36 µm). (Right) Micrograph showing evidence of strong charging when the landing energy is increased to 10 keV, (HFV = 13 µm).*

repeatable. The accumulated charge in the sample material represents a potential energy, and when it is drained, the sample achieves a more neutralized, more stable, less energetic state. Electrical connections, including surface conduction due to humidity, all play a role in discharging the sample. Two major categories of charging can occur:

2.2.2.1 Negative Charging. Negative charge build-up occurs when a number of electrons impinging on the sample are trapped within the material and a negative electrical potential builds up. This can be only few volts or as much as the primary electron beam, i.e., several thousands of volts. The most common manifestation of this situation is that the image appears to "glow" (brighter) or cause geometry distortion in the image as electron production is artificially enhanced or the beam is unintentionally deflected (Figure 1). In other cases, marginally adhered particles can be seen to "blast-off" from the specimen stub – never to be seen again (until they land upon a critical component within the column). Fibers, insect antennae and other protruding structures will also be seen waving at the operator as the beam scans across them.

[3] Low landing energy is used here since that term has replaced the term low accelerating voltage because in some of the newer instruments the electron source can emit electrons at high accelerating voltage, but they are decelerated to a lower landing energy in the column and/or at the sample stage. This technique allows the electron optical column to operate more optimally (see: Reference 1). In SEM literature, landing energy is usually given in kilo-electron volts (keV). For example, 15 kV accelerating voltage with no deceleration results in (approximately) a15 keV energy primary electron beam.

[4] Although, horizontal field width and field of view are often used interchangeably (see: reference 1), HFW has been adopted in this publication since field of view implies a two - dimensional array which is only valid when the beam is normal to the sample (zero degrees of tilt).

Since most samples are not totally conductive, charging is a common situation; a good deal of scientific literature has been devoted to this topic [12 – 14], as well as, the references cited below]. Negative charging is the most evident and troublesome type of charging and under the most extreme circumstances can disrupt and deflect the electron beam, and cause intolerable distortions. One of the first references to this, for the SEM, was Clarke and Stuart [15]. They formulated an explanation for the "formation of the distorted image of the electron collector of the scanning electron microscope when the instrument is used to observe uncoated insulating materials." This was provided as a cautionary note because they correctly felt it could lead to image misinterpretation when uncoated insulating materials were being observed.

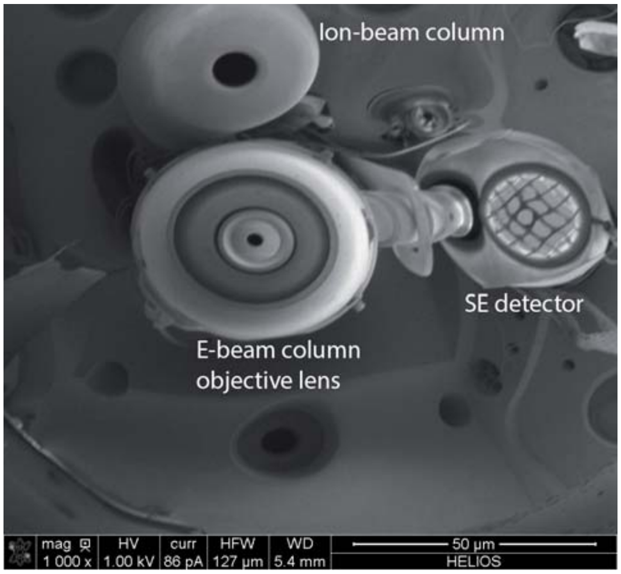


Figure 2. *Example of extreme negative charging causing the primary electron beam to image the inside of the specimen chamber. The instrument "reports" it is scanning a horizontal field width (HFW) of 127 µm however, the stated magnification and HFV recorded on the micrograph are clearly wrong; the HFV is actually approximately 20 cm.*

Figure 2 shows an extreme case of charging resulting in a "mirror microscopy-like" image. In this case, the sample has developed and is retaining a potential at or above that of the primary electron beam. The primary electron beam then does not impinge on the sample as it is scanned over the sample, but it is deflected throughout the specimen chamber generating signal from the internal components of the SEM specimen chamber, such as the final lens, and electron detectors [16, 17]. Even as strange as this mode of instrument operation is, it can also hold a diagnostic function since it can image particles and other contaminants on apertures and the final lens pole piece. Shaffner and Hearle, van Veld and Shaffner, and Shaffner and van Veld [18 – 20], reviewed the phenomenon of charging and also described the mirror mode described above and shown in Figure 2. The extreme negative charging at the sample, causes the primary electron beam to actually become diverted and image the inside of the specimen chamber. Images become grossly distorted and the primary electron beam is deflected as it approaches the sample throughout the chamber when such charging is present. Tilting the sample can direct the beam to various locations of interest. There does not appear to be any negative consequences to these actions, but it is startling to the operator the first time it occurs. This is an amusing application of charging, but this is not the main area where the typical charging problem exists. Typically the majority of problems exist between sample ground and just a few electron volts where subtle, un-recognized charging occurs.

Often, charging is obvious, but sometimes it is quite subtle. Negative charging presents an insidious problem for dimensional measurements because there is the potential for it to deflect the beam such that it actually lands nanometers away from its intended location. The amount of deflection can be negligible or it can be significant depending upon the instrument conditions and the 3-dimensional structure being measured. When the primary beam approaches a charging structure, its trajectory can be altered and the landing point where the signal is being generated and the point where the instrument scanning system believes the landing point can be different, hence leading to erroneous data and measurements. The amount of deflection is variable and depends on the electrical potential, the structure of charging sample, and on the landing energy[3] of the electron beam. This effect was postulated by Postek [21] for photomask metrology and was later demonstrated by Davidson and Sullivan [22] who calculated the electric fields on dielectric materials and showed, with modeling and experimentation that measurements in the SEM could be compromised by several nanometers if charging of only a few volts was occurring on the sample. Further work in this area needs to be done in order to fully understand the uncertainty that such charging poses to the accuracy and of any measurement. However, it is very important to be aware of the potential uncertainty this introduces into the measurement process and to work to eliminate charging in all possible cases.

2.2.2.2 Positive Charging. Positive potential can build up when more electrons are emitted from the sample than the primary electron beam provides. The positively charged regions rather than glowing brighter, get darker, because the secondary electron (SE) emission is reduced, many of the SEs are attracted back to the sample surface. Positive charging turns the scanned area dark and it is often confused with the build-up of contamination (which was discussed in Reference 2). Positive charging is far less detrimental than negative charging, and it is usually restricted only to a few volts of electrical potential. The main result is a loss of some valuable signal electrons as they are re-absorbed by the positively charging surface [23, 24]. Figure 3 shows an interesting effect of the deposition of positive charging on a thin oxide film sample. The initial "writing" of the dark lines was carried out by the automatic exposure (contrast, brightness) setting circuitry that was scanning only over the partial field, resulting in the widely spaced dark scan lines. The acquisition of the final overall image was then taken with that exposure setting. If that sample was allowed to remain in the instrument for a period of time, or removed and put back into the instrument, those dark lines will disappear.

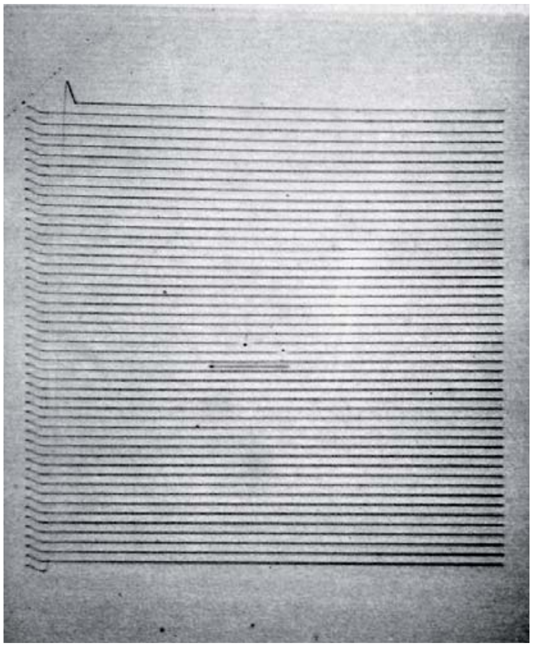


Figure 3. *Positive charging on a thin oxide film sample showing dark lines where the primary electron beam was scanned over the sample during the automatic exposure setting routine. In the case shown, the partial field scanning for the automatic exposure (contrast and brightness) adjustment resulted in positive charging on the portion of the sample exposed by the beam. After the initial adjustment, the final overall image was taken. Note the scan initiation, over-scanning and re-trace can be clearly seen. The micrograph was taken at 1.0 keV (HFW = 2 250 µm).*

2.2.3 Diagnosing Charging. Positive and negative charging can be diagnosed quite easily to determine the proper landing energy and the sample's conductivity:

- Set-up the instrument to the proper instrument operating conditions.
- Locate an area of interest and focus on that area at a high magnification or the magnification where one you plan to do the majority of the work (the effect of charging is exacerbated at higher magnifications).
- Irradiate the sample for a few seconds within the area selected.
- Reduce the magnification by a factor of 5 and observe the sample.
- If a bright raster pattern appears (which may slowly disappear upon going to the lower magnification), negative charging is probable. Therefore, try lowering the landing energy a few 100 eV. Then repeat the procedure at a different location.
- If a dark raster pattern appears, and then (possibly) quickly disappears, positive charging is probable (Figure 3). If that occurs, raise the landing energy a few hundred volts. Then repeat the procedure.
- If the dark square remains, then positive charging is not likely to be the problem. Beam induced contamination is more likely the problem (see: Reference 2).

3.0 Methods for Charge Mitigation

Studies of the phenomenon of sample charging were carried out since early work with the SEM. The SEMs relative similarity to early cathode-ray tube and television research led to many useful and parallel conclusions. The two most common approaches to the mitigation of charging are low accelerating voltage (low landing energy[3]) operation and coating the sample with a thin conductive metal or carbon layer. Other possible solutions are discussed later in Section 3.3.

3.1 Low Accelerating Voltage Observation. Low accelerating voltage (landing energy) operation was possible with most SEMs since the early days, but the imaging was generally poor due to instrument design, poor signal-to-noise ratio and lower resolution [25, 26]. It was not until the latter 1980s when scanning electron microscopes were able to routinely view most samples in a non-destructive, uncoated manner. Many innovative instrument improvements took place which eventually changed instrument operation and the terminology used to low landing energy techniques.[3]. The notable improvements that spurred this was the availability of high brightness electron sources such as lanthanum hexaboride and field emission (and later frame storage electronics which evolved into the current digital imaging electronics). Non-destructive, low landing energy operation became common in semiconductor manufacturing where insulating samples (such as oxides and photoresist) are viewed routinely on the production lines. Early research work in cathode ray tubes and television found that generally, at low landing energies, a charge balance could be achieved when an electron beam impinges on an insulating surface. Thornley [27] reported that at low (1-2 keV) landing energies the secondary electron coefficient could be greater than unity, as shown on Figure 4.

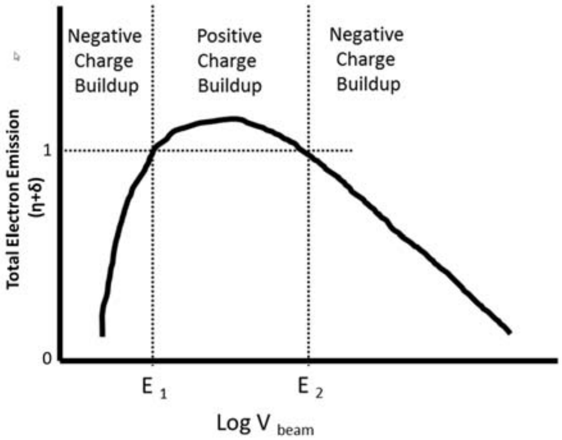


Figure 4. *Total electron emission curve. The E_1 and E_2 points are the landing energies where no sample charging is expected to occur.*

For most non-conductive materials, E_1 and E_2 are the points where the total electron emission is equal to 1. The SEs are not the only electrons that need to be considered, we have also BSE and sample current. For the sample, to be charge balance, all these must come to a stable state. It is thought that these points are relatively stable for a particular sample and set of instrument conditions being applied (landing energy, beam current, tilt, etc.) and they are the energies at which the sample is in charge balance. At that point, the number of electrons injected into the sample by the primary electron beam is equal to the total of those electrons leaving the sample and thus no specimen charging presumably occurs. Usually there is a range of voltages for which a sample can be exposed, up to and including the E_2 value. E_2 is the most stable value and is usually chosen for uncoated observation since it is found at a higher accelerating voltage, thus enabling a higher resolution operating condition for the instrument. However, the optimal landing energy needed is always dependent on the required sample information. A high voltage primary beam will image layers deeper into the sample, while low voltages will provide more information from the sample surface. So compromises must always be optimized. Additionally, newer particle beam instruments with ultra-low voltage/high resolution capability can work acceptably in the E_1 region without significant compromise to the resolution.

3.2 Specimen Coating. Traditionally, over-coating the non-conducting specimen with a heavy metal, conductive, material (gold, gold/palladium, and osmium) has been the most commonly used method to overcome charging. Coating also increases the secondary electron emission from the sample especially if the sample is composed of low atomic number materials (especially biological). The one thing that must be remembered is that, if a sample is coated, signal is mainly being generated from the flux of electrons originating from the coating acting as a protective shell and not necessarily the sample of interest. In addition, a myriad of coating artifacts, such as cracking, can result. Adding the appropriate amount of coating has always been a complicated decision based upon the needed conductivity and the amount of artifacts one can tolerate. Vacuum evaporation (gold, gold/palladium), sputter coating (gold, gold/palladium) and aqueous or vapor deposition of osmium have all been used. The philosophy and techniques can be found in Postek et al,, [28]. For x-ray microanalysis often carbon coating is also helpful in reducing charging and diminishes the effects of stray artifacts in the analysis [29].

A good continuous coating can mitigate charging, but can also introduce coating artifacts such as a change in surface details. Coating also increases the size of the structures being observed relative to the thickness of the coating applied. Therefore, interpretations can be compromised. Figure 5 shows nanocellulose material that has been coated with a deposition of a few nanometers of osmium vapor. Note that the core (observed through the coating) is about the expected 6-7 nanometers in diameter for the cellulose nanomaterial but surrounding it is several additional nanometers of coating. Therefore, coating a nanoparticle potentially compromises the measurements especially on nano-sized particles and structures.

3.3 Other potential solutions. The simplest approach is often the best approach. Hence, non-destructive low accelerating voltage operation is the first method usually applied to an unknown sample. Seasoned microscopists usually begin by applying low landing energies to an unknown sample, unless they know coating will not compromise the imaging or measurements. However, as discussed below, other methods have also been used with varying degrees of success:

3.3.1 Charge Neutralization. Prior to the availability of high resolution imaging at low landing energies, Crawford [30, 31] and others reported good success with specimen charge neutralization. In this case, the charge build-up is neutralized, as it builds up, by a beam of very low energy ions. The ions act to stabilize the surface potential, at the "ion zero kinetic-energy point, independent of the nature of the insulating surface." [30] This requires the installation and optimization of a charge neutralization device in the proximity of the sample. The unit is positioned above the specimen and below the final lens in the specimen chamber of the SEM. Because of the large amount of specimen chamber real estate needed by the device and the prevalence of low landing energy microscopy with high-brightness field-emission instruments, this method is not often practiced, today. In the scanning helium ion microscopes there is an option for an electron flood gun to work to neutralize the positive charging caused by the ions.

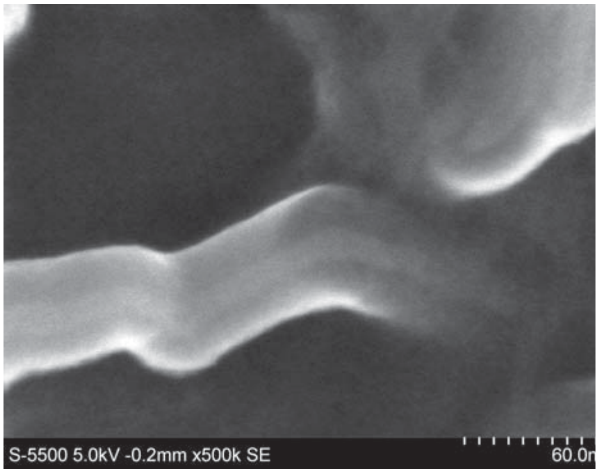


Figure 5. *Micrograph of cellulose nanofibrils that have been coated with osmium vapor in order to reduce the charging. The 6-7 nanometer visible core is likely the cellulose and the remaining thickness is the osmium vapor coating. Images taken at a landing energy of 5 keV (HFV = 316 nm).*

3.3.2 Fast, TV-Rate Imaging. Welter and McKee (1972) [32] demonstrated that fast scanning using a high-brightness field-emission electron microscope could alleviate charging problems. They stated that "if a layer of charge is put down on the specimen and reinforced at a scan rate faster than the average discharge rate," charge equilibrium could be reached. They used a fixed TV scan rate of 1155 lines per frame and 15 frames/sec. and provided reasonable imaging even at low landing energies. This work paved the road for the more modern instruments displaying 60 frames/sec. (or greater). TV-rate imaging is now common on most instruments. But, it took successful demonstration of the concept of fast scanning with good signal-to-noise ratio to prove that charging could be mitigated in this manner.

3.3.3 Backscattered Electron Imaging. One of the earliest approaches to charge mitigation in the SEM was to employ backscattered electron collection rather than secondary electron collection. Charging of the sample affects the secondary electron image far more than the higher-energy backscattered electrons. Most laboratory SEMs are equipped with a mechanism whereby the bias of the collection screen at the front of the SE detector can be grounded or negatively (reverse) biased, thus rejecting the SE and only allowing those high-energy BSEs that are in the proper geometrical relationship to the detector to be collected. Alternatively, dedicated backscattered electron detectors can be employed. Tilting the sample toward the detector is, not only, helpful to improve signal collection and signal strength but also, allow better collection of the BSE. Alternatively, the low loss technique developed by Wells [33] was shown to provide high-resolution images of the sample surface while mitigating the charging.

3.3.3.1 Low-Loss Electron Imaging. Low loss imaging is a subset of backscattered electron imaging where the electrons are energy filtered in such a manner that only those that have minimally interacted with the sample are collected. These are the low loss electrons. These electrons have been demonstrated to have greater surface sensitivity and reduced apparent charging [34 – 37]. Overall, sample charging is not eliminated and beam deflection by surface charging can still occur - the charging is not dissipated, just ignored. If the charge builds up sufficiently, deflection of the primary electron beam is still possible.

3.3.4 Conductive Spray. Prior to the prevailing use of high-resolution low landing energy microscopy, experiments were undertaken to use a "conductive" spray to eliminate charging. As early as 1957, Wells [11] described experiments with several potential anti-static materials. It is notable that, conductive spray was reported to be successfully used on polymers by Sikorski et al. (1967) [38] to view polymers with no or reduced charging at high landing energies. A “conductive film aerosol” was marketed in 1980, as a commercial product, but was taken off the market several years later. A similar product has been recently revived as ConductCoat [39]. This product appears to have some success in reducing charging on some materials, but an overall comparison if this material to low landing energy operation has not been done, nor have the effects on instrument or specimen contamination been fully studied.

3.3.5 Variable Pressure SEM. It is clear that, charging must be overcome in order to obtain any meaningful data from the SEM. Gross charging can readily distort the image and subtle charging can deflect the beam and lead to measurement error. An alternative that has not been fully explored for metrology is the employment of variable pressure or “environmental” microscopy [40 – 43]. This methodology uses a gaseous environment to neutralize the charge. For various technical reasons, high-pressure microscopy has mostly been employed for specimens of a biological nature, not for many semiconductor samples. Figure 6 shows several images of photomask samples taken at high landing energies usingt variable pressure technoloogy demonstrating no charge accumulation. Photomasks are very prone to charging [44]. It has been reported that high accelerating voltage, injection of air of as little as 20 Pa ~0.15 Torr into the specimen chamber can reduce the charging potential of an insulator at the surface by as much as an order of magnitude [45]. For accurate metrology, this methodology affords a path that minimizes, if not eliminates, the need for charge modeling. Modeling of charging is exceptionally difficult since each sample, instrument and operating mode can respond to charging in different ways. This methodology shows great potential if optimal balance can be achieved in a reproducible manner. This methodology, although potentially desirable for charge neutralization, has not been seriously employed in photomask or wafer metrology [46]. This is largely because there is not an instrument available for full-scale production samples with high throughput. VPSEM was proven to be useful for photomask metrology [46] but no in-line instrument was developed to use the technology, either. Variable pressure microscopy offers advantages of possible application of higher accelerating voltages and different contrast mechanisms [47].

4.0 ADVANTAGES OF SAMPLE CHARGING

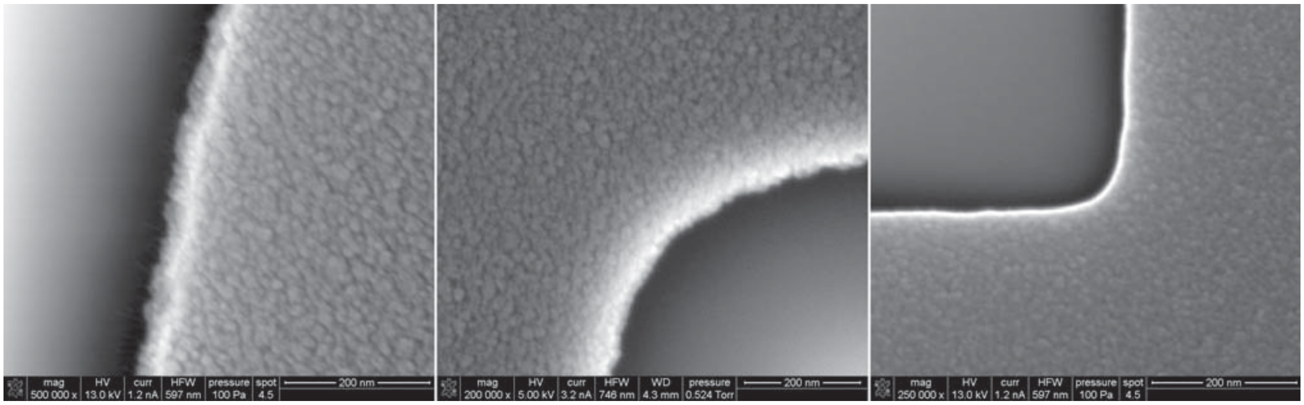

mag HV curr HFW pressure spot
500 000 x 13.0 kV 1.2 nA 597 nm 100 Pa 4.5
200 nm
mag HV curr HFW WD pressure
200 000 x 5.00 kV 3.2 nA 746 nm 4.3 mm 0.524 Torr
200 nm
mag HV curr HFW pressure spot
250 000 x 13.0 kV 1.2 nA 597 nm 100 Pa 4.5
200 nm

Figure 6. *SEM Micrographs of several chromium photomask samples using the variable pressure SEM. (Left) 13 keV landing energy (HFW =597 nm); (Center) 5keV landing energy (HFW = 746 nm); (Right) 13 keV landing energy (HFW =597 nm).*

On the other side of the coin, charging can be used and advantageously controlled. Charge contrast forms the basis of several imaging modes such as voltage contrast (VC) and electron beam induced conductivity (EBIC). Both of these methods are used extensively in semiconductor electronics testing and quality control [23, 48, and 49].

4.1 Charge Contrast. More recently, some conductive materials buried on non-conducting matrices have been shown to be successfully imaged using charge induced contrast. Properly choosing the instrument operating conditions, sub-surface

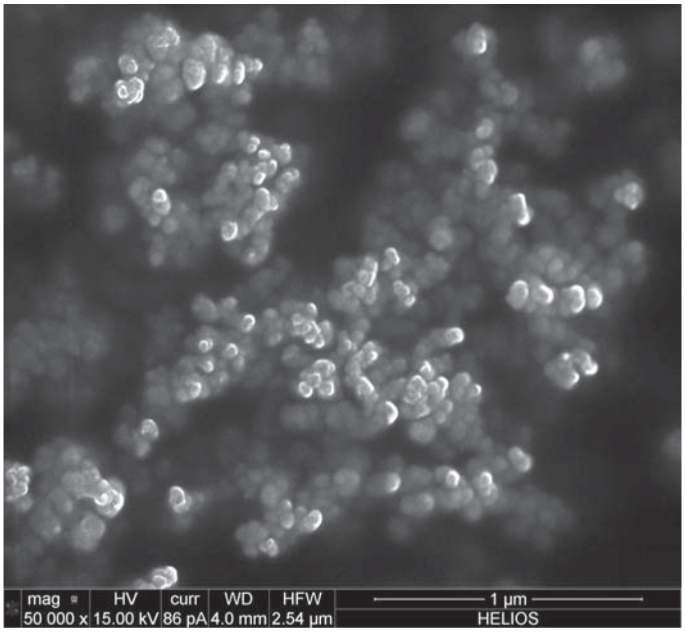


Figure 7. *Micrograph of tangled multiwall CNT structures in an epoxy matrix taken at 15keV (HFW = 2.54 µm) those that are sharper reside close to the surface and others are several nanometers below the surface.*

imaging of materials, such as carbon nanotubes (CNT) in polymers (epoxy) can be imaged embedded as deeply as several 100 nm [50, 51]. Figure 7 shows an example of tangled multiwall CNT structures that reside close to the surface and also images those deeper in the matrix.

5.0 CONCLUSION

Charging is an inevitable consequence of particle beam microscopy of non-conductive samples. It is clear that charging must be overcome in order to obtain meaningful and repeatable data from the SEM. Coating of the sample to make it conductive is only one solution, which could lead to artifacts. Gross charging readily distorts the image and subtle charging can deflect the beam and hence can lead to measurement error. Charging can be overcome with judicious application of the methods discussed in this presentation. For general imaging, charging can be useful and it may create interesting micrographs, but for measurements it can lead to a great deal of error if the operator is not careful.

6.0 REFERENCES

[1] Postek, M. T., Vladár, A. E., “Does Your SEM Really Tell the Truth? How would you know? Part 1,” SCANNING 35:355-361 (2013).

[2] Postek, M. T., Vladár, A. E., Kavuri, P. P., “Does Your SEM Really Tell the Truth? How would you know? Part 2. Specimen Contamination,” SCANNING 36:347-355 (2014).

[3] Postek, M. T., Vladár, A. E., and Cizmar, P., “Nanomanufacturing Concerns about Measurements made in the SEM Part III: Vibration and Drift,” SPIE 9173 917306 pp. 1 to 10 (2014).

[4] Postek, M. T., Vladár, A., “Modeling for Accurate Dimensional Scanning Electron Microscope Metrology: Then and Now,” SCANNING 33: 111-125 (2011).

[5] Postek, M. T., Vladár, A. E. Lowney, J., Larrabee, R. D. and Keery, W. J., “Two- Dimensional Simulation and Modeling in Scanning Electron Microscope Imaging and Metrology Research,” SCANNING 24:179-185 (2002).

[6] Rose, A. and Iams, H., “Television pickup tubes using low-velocity electron-beam scanning,” Proc. I. R. E. 547- 555 (1939).

[7] Zworykin, V. K., Morton, G., and Malter, L., "The secondary emission multiplier – a new electronic device," Proc. Inst. Radio Eng. 24(3) 351- 375 (1936).

[8] Zworkyin, V. A. and Morton, G., "Television: The electronics of image transmission," John Wiley and Sons New York, 646 (1945).

[9] Zworykin, V. A. Hillier, J and Snyder R., "A scanning electron microscope," ASTM Bulletin 117:15-33 (1942).

[10] McMullan, D., "Investigations relating to the design of electron microscopes," Dissertation Univ. of Cambridge 202 pp. (1952).

[11] Wells, O. C., "The construction of a scanning electron microscope and its application to the study of fibres," Dissertation Univ. of Cambridge, 153pp (1957).

[12] Lau, K. M., Drouin, D., Lavallée, E., and Beauvais, J., "The Impact of Charging on Low-Energy Electron Beam Lithography," Microscopy and Microanalysis, 10, pp 804- 809 (2004).

[13] Anger, K., Lischke, B., and Sturm, M., "Material surfaces for electron-optical equipment," SCANNING 5:39-44 (1983).

[14] Reimer, L., Golla, U., Böngler, R., Kassens, M., Schindler, B., and Senkel, R., "Charging of bulk specimens, insulating layers and free-supporting films in scanning electron microscopy," Optik 92(1) 14-22 (1992).

[15] Clarke, D. R. and Stuart, P. R., "An anomalous contrast effect in the scanning electron microscope," J. Phys. E: Sci. Instrum. 3: 705-707, (1970).

[16] Alvarez, A, Bonetto, R. Guerin, D., and Peez, C., "Images of the inner parts of scanning electron microscopes," Electron Optics Reporter (Norelco) 31:1EM 39-43 (1984).

[17] Eckert, R., "Inspecting the SEM Chamber with a charged polystyrene mirror," SCANNING 14:73-75 (1992).

[18] Shaffner, T. J. and Hearle, J. W. S., "Recent advances in understanding specimen charging. Scanning Electron Microscopy/1976 (Part 1)," IITRI Chicago, IL 60616 61-70 (1976).

[19] Van Veld, R. D., and T. J. Shaffner, "Charging effects in scanning electron microscopy." Scanning Electron Microscopy/1971, 19-24 IITRI, Chicago, Il 60616 (1971).

[20] Shaffner T. J., and van Veld R. D., "Charging effects in the scanning electron microscope," J. Phys. E Scientific Instruments 4(9): 633-637 (1971).

[21] Postek, M. T., "Low Accelerating Voltage Inspection and Linewidth Measurement in the Scanning Electron Microscope," SEM/1984/III, SEM, Inc. 1065-1074 (1984).

[22] Davidson, M. and Sullivan, N, "An investigation of the effects of charging in SEM based CD metrology," Proc. SPIE 3050 226-252 (1997).

[23] Postek, M. T. and Joy, D. C., "Submicrometer Microelectronics Dimensional Metrology: Scanning Electron Microscopy," NBS Journal of Research 92 (3): 205-228 (1987).

[24] Postek, M. T., "Critical Issues in Scanning Electron Microscope Metrology," NIST J. Res. 99(5): 641-671 (1994).

[25] Blake, D. F., "Low voltage scanning electron microscopy." Test and Measurement. World, 6:62-75 (1986).

[26] Mullerova, I. and Lenc. M., "Some approaches to low-voltage scanning electron microscopy," Ultramicroscopy 41(4) 399-410 (1992).

[27] Thornley, R. F. M., "Recent developments in scanning electron microscopy," Proc. European Regional Conf. on Elect. Microscopy Delft, Vol. 1 (Nederland Verein Electronen) pp. 173-176 (1960).

[28] Postek, M.T., Howard, K.S., Johnson, A.J., and McMichael, K., "Scanning Electron Microscopy - A Student Handbook," Ladd Research Industries, 305 pp (1980).

[29] Bastin, G. F. and Heijigers, H., "Quantitative electron probe microanalysis of non-conducting specimens: science or art?" Microscopy & Microanalysis, 10: 733-738 (2004).

[30] Crawford, C. K., "Charge neutralization using very low energy ions" SEM/1979/II SEM Inc., AMF O'Hare, Il 60666, 31-46 (1979).

[31] Crawford, C. K., "Ion charge neutralization effects in scanning electron microscopes," SEM/1980/IV SEM Inc., AMF O'Hare, IL 60666, 11-25 (1980).

[32] Welter, L. M., and McKee, A. N., "Observations on uncoated, non-conducting or thermally sensitive specimens using a fast scanning field emission source SEM," SEM1972 IITRI Chicago, Ill 60616 161-168 (1972).

[33] Wells, O. C., "Low-loss Image for Scanning Electron Microscope," Appl. Phys. Lett. 19(7): 232-235 (1971).

[34] Wells, O. C., "Low-loss Electron Images of Uncoated Photoresist in the Scanning Electron Microscope," Appl. Phys. Lett. 49(13): 764-766 (1986).

[35] Wells, O. C., "Low-loss Electron Images of Uncoated Non-Conducting Samples in the Scanning Electron Microscope," Microbeam Analysis/1987 (Geiss, R. H., ed.) San Francisco Press, San Francisco CA. 76-78 (1987).

[36] Wells, O. C. and Rishton, S. A. "Studies of Poorly Conducting Samples by the Low-Loss Electron Method in the Scanning Electron Microscope" Proc. 52nd. Annual Meeting MSA, Bailey, G. W. and Garratt-Reed, A. J., Eds. 1022-1023 (1994).

[37] Postek, M. T., Vladár, A. E., Wells, O. C., and Lowney, J. L., "Application of the low- loss scanning electron microscope SEM image to integrated circuit technology. Part 1. Applications to accurate dimension measurements," Scanning 23(5): 298–304 (2001).

[38] Sikorski, J., Moss J. S., Newman P.H, and Buckley, T., "A new preparation technique for examination of polymers in the scanning electron microscope," J. Phys. E 2(1):29-31 (1968).

[39] Burnett, B., "An electro-conductive organic coating for scanning electron microscopy" SPIE Vol. 9236 92360L – 1 - 9236 92360L-9 (2014).

[40] Danilatos, G., "Foundations of environmental scanning electron microscopy," Adv. Electron. Electron Phys. 71, 109–250 (1988).

[41] Danilatos, G., "Introduction to the ESEM instrument," Microscopy Res. Tech. 25, 354–361 (1993).

[42] Donald, A., "The use of environmental scanning electron microscopy for imaging of wet and insulating materials," Nature Materials 2: 511-516 (2003).

[43] Thiel, B. and Toth, M. "Secondary electron contrast in low-vacuum environmental scanning electron microscopy of dielectrics," J. Appl. Phys. 97 051101-1 – 051101-18 (2005).

[44] Postek, M. T. and Vladár A. E., "New application of variable pressure/environmental microscopy to semiconductor inspection and metrology," SCANNING 26:11-17 (2004).

[45] Joy, D. C., "The future of e-beam metrology: Obstacles and opportunities," Proc. SPIE 4689, 1–10. (2002).

[46] Postek, M. T, Vladár, A. E., and Bennett, M., "Photomask dimensional metrology in the scanning electron microscope, Part 1: has anything really changed?" JM3 3(2): 212- 223 (2004).

[47] Postek, M. T. and Vladár, A.E., "Critical dimension metrology in the scanning electron microscope," in Handbook of Silicon Semiconductor Metrology, (edited by A. Diebold, Dekker, New York), Chap. 14, pp. 295–333 (2000).

[48] Feuerbaum, H. P., "Electron beam testing: methods and applications," Scanning 5:14-24 (1983).

[49] Leamy, H., "Charge collection scanning electron microscopy" J. App. Phys. 53 (R51-R80) (1982).

[50] Finnie, P., Kaminska, K., Homm, Y., Austing, D., Lefebvre, J., "Charge contrast imaging of suspended nanotubes by scanning electron microscopy, Nanotechnology 19: 335202 (6pp) (2008).

[51] Zhao, M., Ming, B., Kim, J-W, Gibbon, L., Gu, X., Nguyen, T., Park, C., Lillehei, P., Villarrubia,,J., Vladár, A. E., and Liddle, J. A., "New insights into subsurface imaging of carbon nanotubes in polymer composites via scanning electron microscopy," Nanotechnology 26: 085703 12pp (2015).

Thermometry with Optomechanical Cavities

Thomas P. Purdy[1]***, Karen E. Grutter**[2]**, Kartik Srinivasan**[2]**,**
Nikolai N. Klimov[1,3]**, Zeeshan Ahmed**[3]**, Jacob M. Taylor**[1,4]
[1]*Joint Quantum Institute, National Institute of Standards and Technology, Gaithersburg, Maryland 20899, USA*
[2] *Center for Nanoscale Science and Technology, National Institute of Standards and Technology, Gaithersburg, MD 20899 USA*
[3]*Thermodynamic Metrology Group, Sensor Science Division, Physical Measurement Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899*
[4]*Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD 20742, USA*
**thomas.purdy@nist.gov*

Abstract: The thermally-driven motion of a nanomechanical resonator may be employed as an absolute thermometer. We experimentally measure radiation pressure shot noise induced quantum correlations to absolutely calibrate the motional signal transduced onto an optical probe.

OCIS codes: Quantum optics: 270.0270; Instrumentation, measurement, and metrology: 120.6780 Temperature; Quantum optics: 270.5290 Photon statistics.

Nano-optomechanical systems are promising sensors for a wide variety of physical quantities from force, acceleration, and displacement to mass, pressure, and temperature. Here, we focus on thermometry with on-chip optomechanical systems. The basic concept is that the average mean square thermally-driven Brownian motion of a nanomechanical resonator is proportional to the absolute temperature of the sample. This motion is read out with a cavity enhanced optical probe. Once the mechanical to optical transduction factor is ascertained, this system can serve as an on-chip photonic temperature standard. Pairing this standard with on-chip thermometers such as silicon photonic cavities [1, 2], whose large thermo-optical coefficient makes them fast and sensitive, will create robust, field-calibratable devices with all optical addressing.

Determining the mechanical-to-optical transduction factor is vital for accurate thermometry and is experimentally challenging, typically requiring detailed knowledge of the system parameters such as the mechanical resonator effective mass, optomechancial coupling rate, optical cavity decay rate, and optical losses. However, methods such as taking the ratio of the anti-Stoke to Stokes Raman scattering rate in material [3] or engineered optomechanical systems [4, 5] provides a fundamental, parameter-free calibration. This ratio is given by $n_m/(n_m+1)$ in the limit of small Stokes shift, where n_m is the average phonon occupation number of the mechanical mode. Using linear optical detection, e.g. optical heterodyne, Raman ratio techniques amount to measuring the quantum correlations induced on the output by the optomechanical interaction [6, 7]. Common additional complications with Raman ratio techniques include correctly accounting for the optical density of states at the anti-Stokes and Stokes scattering frequencies, especially if narrowband optical resonant enhancement is employed and unraveling detector dispersion and nonlinearity. To address these and other systematic effects, we investigate techniques such as driving the mechanics with an additional coherent force to act as a classical calibration tone and cross correlation measurements [8-10].

Our system consists of a silicon nitride optomechanical crystal [11] (Fig. 1), chosen for its relatively high mechanical resonance frequency, and consequently small n_m. A suspended nanobeam waveguide is patterned with holes that act as Bragg scatterers for both acoustic and optical waves. A defect is introduced into the periodic hole array to create colocalized acoustic and optical resonances with a strong optomechanical interaction. The silicon nitride optomechanical crystal is evanescently coupled to a tapered optical fiber to allow for optical addressing. Two optical modes with differing resonant wavelengths are addressed with two separate lasers, but both are optomechanically coupled to the same mechanical resonator. One mode is driven with strongly amplitude modulated light to provide a coherent force on the mechanics. The other mode is driven resonantly with a shot-noise-limited laser, and serves as the optical readout of the mechanics. Light collected from this mode is detected with optical heterodyne. From the heterodyne signal, we can compute either the power spectrum of the heterodyne signal, giving direct access to the anti-Stokes and Stokes scattering peaks (Fig. 2(a)), or digitally mix down the photodiode signal to simultaneously access one or more optical quadratures (Fig. 2(b)), allowing for quadrature cross correlation measurements. Computing the spectrum of correlations between two carefully chosen orthogonal optical quadratures reveals the radiation pressure shot noise induced quantum correlations free from additional background signals. The size of this correlation provides the calibrated increment for absolute thermometry.

These types of measurements are quite demanding for megahertz [4] and gigahertz [5] frequency mechanical resonators and have been performed previously only at cryogenic temperatures and with additional

Purdy, Thomas; Grutter, Karen; Srinivasan, Kartik; Klimov, Nikolai; Ahmed, Zeeshan; Taylor, Jacob.
"Thermometry with Optomechanical Cavities."
Paper presented at the OSA Conference on Lasers and Electro-optics (CLEO), San Jose, CA, Jun 5-Jun 10, 2016.

optical cooling. For example, at room temperature, the average mechanical phonon occupation, n_m, of our 3.6 GHz mechanical resonator is about 1700 quanta, meaning that the difference between the anti-Stokes and Stokes scattering peaks is only about $1/n_m$, or equivalently the quantum correlations are buried under uncorrelated noise on the order of n_m times larger. However, our measurement techniques should allow us to discern these small effects from cryogenic to room temperature. Our preliminary experimental results demonstrate the direct measurement of optomechanically-induced quantum correlations over a wide temperature range.

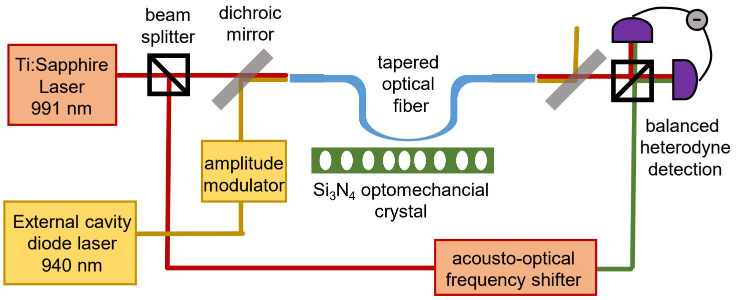

beam splitter
dichroic mirror
Ti:Sapphire Laser 991 nm
tapered optical fiber
amplitude modulator
Si_3N_4 optomechancial crystal
balanced heterodyne detection
External cavity diode laser 940 nm
acousto-optical frequency shifter

Fig. 1 Experimental Setup. Two lasers resonant with two optical modes of the Si_3N_4 optomechanical crystal are combined on a dichroic mirror and sent through a tapered optical fiber evanescently coupled to the optomechanical crystal. One laser is amplitude modulated at the mechanical resonance frequency to provide a coherent optical force. A portion of the other laser is split off and frequency shifted to serve as a local oscillator. After interacting with the cavity, the second beam and frequency shifted local oscillator are interfered to perform balanced heterodyne detection of the optomechanical Raman sidebands on the second beam.

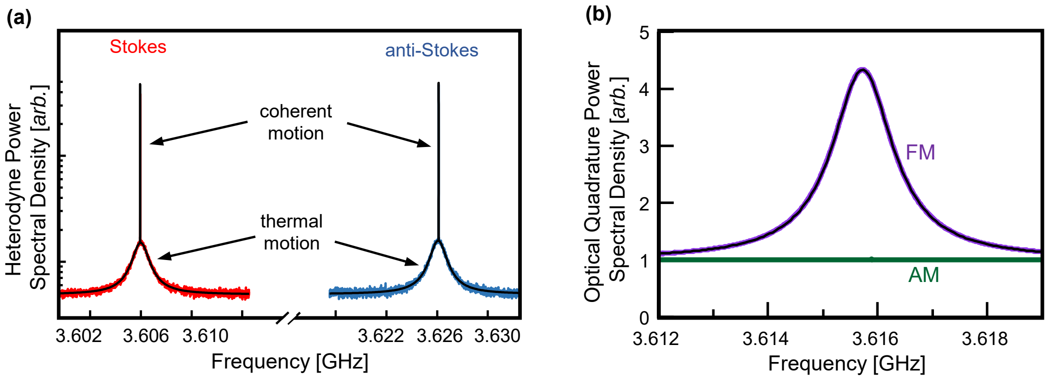


Fig. 2. (a) Heterodyne power spectrum of mechanical sidebands. Lorentzian components are indicative of thermal motion. Sharp peaks are the result of optically driven coherent motion. Anti-Stokes sideband is blue. Stokes sideband is red. Fits are black. (b) Optical quadrature spectrum resulting from digitally mixing down heterodyne signal for an on resonant optical probe. Frequency quadrature (FM) is purple and shows Lorentzian spectrum of thermally driven motion. Amplitude quadrature (AM) is green and is dominated by shot noise. For both plots the parameters are: temperature 294 K, optical resonance wavelength 991 nm, optical linewidth ≈10 GHz, mechanical resonance frequency 3.616 GHz, mechanical linewidth 1.3 MHz, optomechanical cooperativity<<1, heterodyne local oscillator offset frequency 10 MHz.

References

[1] H. Xu, *et al*., "Ultra-sensitive chip-based photonic temperature sensor using ring resonator structures," Optics Express, **22**, 3098 (2014).
[2] N. N. Klimov, *et al*., "On-Chip Integrated Silicon Photonic Thermometers," Sensors & Transducers, **191**, 67 (2015).
[3] J. P. Dakin, *et al*., "Distributed Anti-Stokes Ratio Thermometry," in Optical Fiber Sensors (Optical Society of America, Washington, D.C., 1985), paper PDS3.
[4] T. P. Purdy, *et al*., "Optomechanical Raman-Ratio Thermometry," Phys. Rev. A, **92**, 031802 (2015).
[5] A. Safavi-Naeini, *et al*., "Measurement of the quantum zero-point motion of a nanomechanical resonator," Phys. Rev. Lett. **108**, 033602 (2012)
[6] F. Y. Khalili, *et al*., "Quantum back-action in measurements of zero-point mechanical oscillations," Phys. Rev. A, **86**, 033840, (2012).
[7] A. J. Weinstein, *et al*., "Observation and interpretation of motional sideband asymmetry in a quantum electro-mechanical device," Phys. Rev. X, **4**, 041003, (2014).
[8] A. Heidmann, Y. Hadjar, M. Pinard, "Quantum nondemolition measurement by optomechanical coupling," Appl. Phys. B, **64**, 173 (1997).
[9] K. Børkje, *et al.*, "Observability of radiation-pressure shot noise in optomechanical systems," Phys. Rev. A, **82**, 013818 (2010).
[10] T. P. Purdy, R. W. Peterson, C. A. Regal, "Observation of Radiation Pressure Shot Noise on a Macroscopic Object," Science **339**, 801 (2013).
[11] K. E. Grutter, M. Davanco, K. Srinivasan, "Si_3N_4 nanobeam optomechanical crystals," IEEE J. Sel. Topics Quantum Electron, **21**, 2700611 (2015).

Purdy, Thomas; Grutter, Karen; Srinivasan, Kartik; Klimov, Nikolai; Ahmed, Zeeshan; Taylor, Jacob.
"Thermometry with Optomechanical Cavities."
Paper presented at the OSA Conference on Lasers and Electro-optics (CLEO), San Jose, CA, Jun 5-Jun 10, 2016.

CHARACTERIZING THE THERMAL EFFECTS OF HIGH ENERGY ARC FAULTS

Anthony Putorti[1], Nicholas B. Melly[2], Scott Bareham[1], Joseph Praydis Jr.[1]

[1] National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA
[2] U.S. Nuclear Regulatory Commission (NRC), Washington, DC, USA*

ABSTRACT

International and domestic operating experience involving High Energy Arc Faults (HEAF) in Nuclear Power Plant (NPP) electrical power systems have demonstrated the potential to cause extensive damage to electrical components and distribution systems along with damage to adjacent equipment and cables. An international study by the Committee on the Safety of Nuclear Installations (CSNI) “OECD Fire Project – Topical Report No. 1: Analysis of High Energy Arcing Fault (HEAF) Fire Events” published June 25, 2013 [1], illustrates that HEAF events have the potential to be major risk contributors with significant safety consequences and substantial economic loss. In an effort to better understand and characterize the threats posed by HEAF related phenomena, an international project has been chartered; the Joint Analysis of Arc Faults (Joan of ARC) OECD International Testing Program for High Energy Arc Faults. One of the major challenges of this research is how to properly measure and characterize the risk and influence of these events. Methods are being developed to characterize relevant parameters such as; temperature, heat flux, and heat release rate of fires resulting from HEAF events. Full scale experiments are being performed at low (≤ 1000 V) and medium (≤ 35 kV) voltages in electrical components. This paper introduces the methods being developed to measure thermal effects and discusses preliminary results of full scale HEAF experiments.

INTRODUCTION

Switchgear, load centers, and bus bars/ducts (440 V and above) are subject to a unique failure mode and, as a result, unique fire characteristics. In particular, these types of high-energy electrical devices are subject to high-energy arcing fault (HEAF). This fault mode leads to the rapid release of electrical energy in the form of heat, vaporized copper/aluminum, and mechanical force. Faults of this type are also commonly referred to as high energy, energetic, or explosive electrical equipment faults or fires.

The energetic fault scenario typically consists of two distinct phases, each with its own damage characteristics. The first phase is characterized by a short, rapid release of electrical energy which may result in catastrophic failure of the electrical enclosure, ejection of hot projectiles (from damaged electrical components or housing) and/or fire(s) involving the electrical device itself, as well as any external exposed combustibles, such as overhead exposed cable trays or nearby panels, that may be ignited during the energetic phase. The second phase, i.e., the ensuing fire(s) typically includes ignition of combustible material within the HEAF zone of influence (ZOI). The resulting fire may be due to the ejection of hot particles or piloted ignition of combustibles. HEAF events are of concern due to their potential to im-

* This paper was prepared (in part) by employees of the United States Nuclear Regulatory Commission. It presents information related to NRC upcoming testing programs. NRC has neither approved nor disapproved its technical content. This paper does not establish an NRC technical position.

pact adjacent items important to safety and current limitations in characterizing the ZOI as defined in NUREG/CR-6850 [2].

Due to the potential safety significance of HEAF events, the OECD (*O*rganization for *E*conomic *C*o-operation and *D*evelopment) Nuclear Energy Agency (NEA) Integrity and Ageing Working Group (IAGE) initiated a task on High Energy Arcing Events (HEAF) in 2009 to provide an in-depth investigation on HEAF events in NEA member states [3]. The objective of this working group is to determine damage mechanisms, extent of areas affected, methods of protecting systems, structures and components (SSC) and possible calculation methods for modeling of HEAF events as applicable to fire protection in nuclear power plants (NPP). As part of this effort a testing program has been initiated to investigate the HEAF fire phenomena to inform future deterministic and probabilistic methods.

This paper presents methods for measuring the heat release rates of ensuing fires and measuring the heat fluxes above and around the electrical enclosures during the HEAF experimental program. Limited data are also presented.

BACKGROUND

In order to characterize the effects of the HEAF and ensuing fire on the surrounding equipment, various phenomena were chosen for characterization in the OECD program. These include enclosure pressure, enclosure surface temperature, heat release rate, and heat flux to target equipment. Electrical test parameters such as arc voltage, arc current, and arc duration were also measured during the experiments.

Experiments were performed at KEMA-Powertest, located outside of Philadelphia, Pennsylvania, USA. The test facility includes a five-sided test cell approximately 8 m (26 ft) high, 7 m (24 ft) deep, and 9 m (29 ft) wide. The sixth side of the test cell includes a roll-up door that was fully open during the experiments. Bus bar connections for supplying low and medium voltage test current are located on opposite side walls of the test cell. KEMA-Powertest provided measurements of electrical enclosure pressure, temperatures of slug calorimeters, electrical test parameters, videography, and high speed videography during the experiments. NIST provided measurements of heat release rate, heat flux, electrical enclosure surface temperature, thermal imaging, and multiple location videography during the experiments.

The NPP equipment for the experiments was provided by OECD/NEA HEAF Project partners. Fourteen experiments have been performed to date using six electrical enclosures. Nominal test voltages ranged from 480 VAC to 7200 VAC, and nominal test currents ranged from 24 kA to 50 kA. All of the experiments conducted thus far have been performed with three phase power supplied in a delta configuration. The arcs were initiated in the enclosures by shorting across all three bus bar phases with a 2.6 mm diameter (10 AWG) tinned copper stranded wire prior to energizing the enclosures.

EXPERIMENTAL METHODS

Heat Release Rate

In order to measure the heat release rate (HRR) of the ensuing fires caused by the HEAF events, a portable oxygen consumption heat release rate hood apparatus was deployed. The portable hood was first used in the HELEN-FIRE experiments to measure the heat release rates of fires in control cabinets as described in NUREG/CR-7197 [4]. The portable apparatus was further developed and refined for use in the HEAF experiments. In the current form, the apparatus is a portable stand-alone system resistant to the effects of electromagnetic interference (EMI).

The portable hood, installed in the HEAF test cell with an electrical enclosure, is shown in Figure 1 and Figure 2. The hood was approximately 2.44 m by 2.44 m in width, with a clear height of approximately 3.0 m above the floor. Side skirts constructed of fiberglass welding curtain hung around the hood opening to reduce the quantity of smoke that escaped from the sides of the hood.

The exhaust duct exiting the top of the hood is approximately 0.46 m in diameter, and carries air and combustion products through flow measurement, gas sampling, and exhaust fan sections. The ducting is supported by scaffolding (not shown). The distance between the hood and the flow measurement section was varied with additional duct sections (not shown) to provide adequate clearance between the electrical enclosures and the metal scaffolding. The hood exhaust fan motor was powered by a dedicated portable electrical generator located outside of the test cell. The gas analyzers and data acquisition system were located in an interior hallway outside the rear of the test cell for protection from physical hazards, electrical hazards, and combustion products.

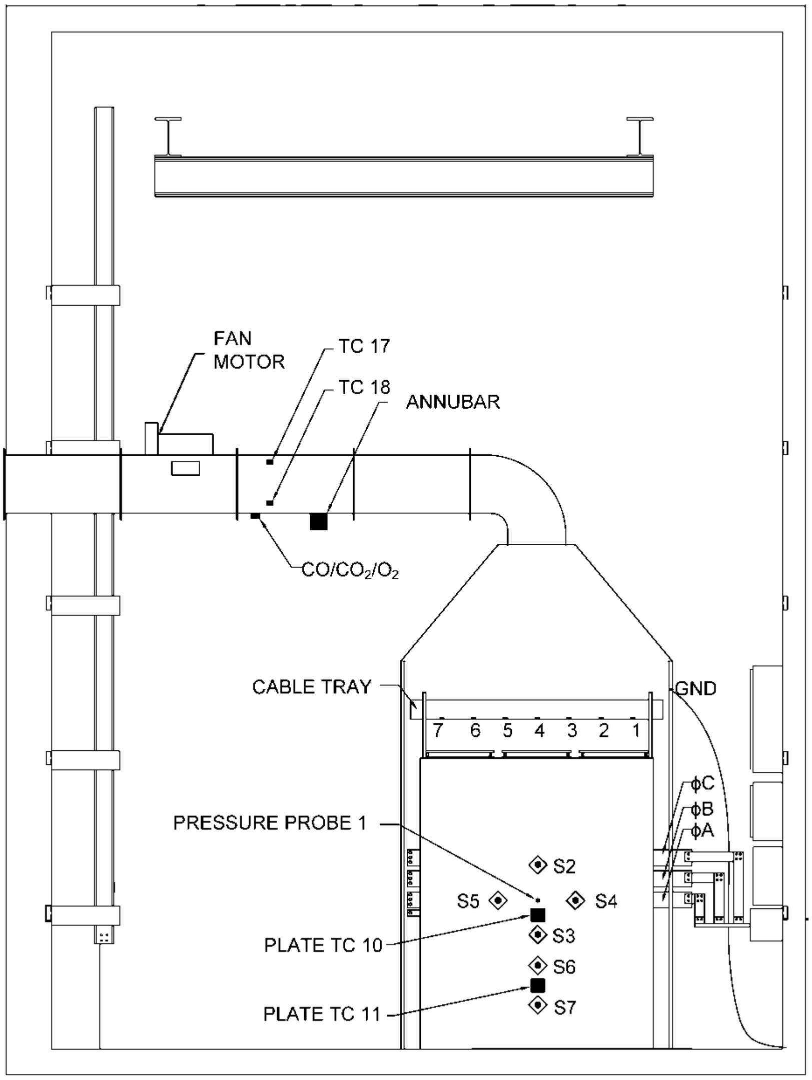


Figure 1 Elevation view of calorimetry hood, enclosure, and instrumentation. Plate thermometers facing downward under cable tray, slug calorimeters denoted by diamond symbols, stack thermocouples denoted by "TC", exhaust gas sampling probe location denoted by "CO/CO$_2$/O$_2$"; earth ground cable attached to hood denoted "GND", bus bars labeled with phases A, B, and C; not to scale

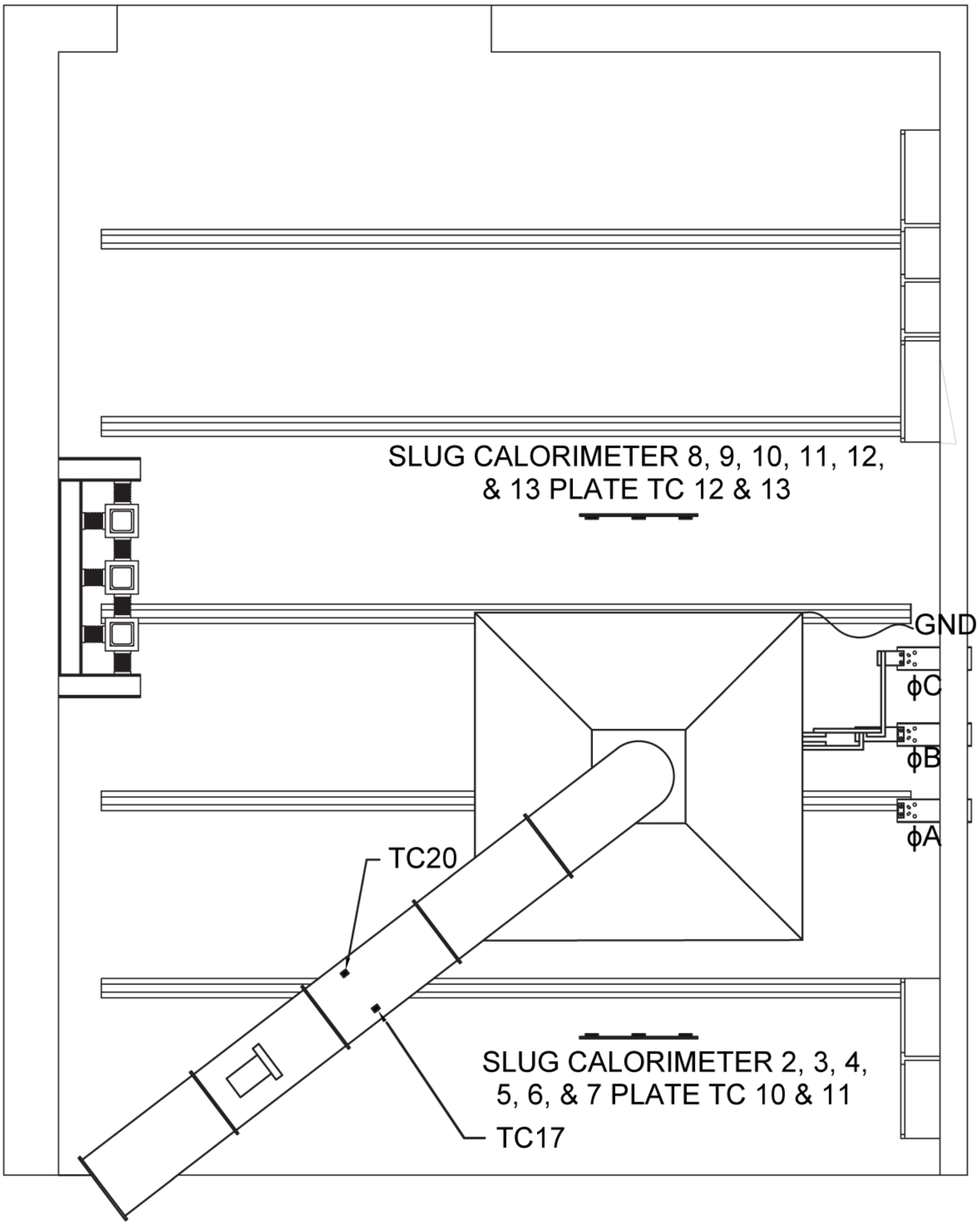

SLUG CALORIMETER 8, 9, 10, 11, 12, & 13 PLATE TC 12 & 13
GND
ϕC
ϕB
ϕA
TC20
SLUG CALORIMETER 2, 3, 4, 5, 6, & 7 PLATE TC 10 & 11
TC17

Figure 2 Plan view of calorimetry hood, cabinet, and instrumentation; not to scale

The heat release rates of the ensuing fire, $\dot{Q}(t)$ (kW), was measured by oxygen consumption calorimetry, taking into account the measured concentrations of oxygen, carbon dioxide, and carbon monoxide in the exhaust gas [5], [6].

$$\dot{Q}(t) = \left[E_{O_2}\emptyset - \left(E_{CO} - E_{O_2}\right)\frac{1-\emptyset}{2}\left(\frac{X_{CO}}{X_{O_2}}\right)\right]\frac{\dot{m}_e}{1+\emptyset(\propto -1)}\frac{M_{O_2}}{M_a}\left(1 - X_{H_2O,\infty}\right)X_{O_2,\infty} \quad (1)$$

$$\emptyset = \frac{X_{O_2,\infty}\left(1 - X_{CO_2} - X_{CO}\right) - X_{O_2}\left(1 - X_{CO_2,\infty}\right)}{\left(1 - X_{O_2} - X_{CO_2} - X_{CO}\right)X_{O_2,\infty}} \quad (2)$$

Here $\propto$ is the combustion expansion factor of 1.105, $\emptyset$ is the oxygen depletion factor, E_{O_2} is the net heat released for complete combustion of typical fuels, 13100 kJ/(kg O$_2$), E_{CO} is the net heat released for complete combustion of CO, 17600 kJ/(kg O_2), M_a is the molecular weight of incoming air [g/mol], M_{O_2} is the molecular weight of oxygen [g/mol], $\dot{m}_e$ is the exhaust mass flow rate in the duct [kg/s], $X_{O_2,\infty}$ is the initial oxygen volume fraction, X_{O_2} is the measured oxygen volume fraction, $X_{CO_2,\infty}$ is the initial carbon dioxide volume fraction, X_{CO_2} is the measured carbon dioxide volume fraction, X_{CO} is the measured carbon monoxide volume fraction, and $X_{H_2O,\infty}$ is the volume fraction of water vapor.

Due to the large range of possible heat release rates, the apparatus design was biased toward resolution of the relatively small heat release rates expected from the ensuing fires. The heat release rate measurement range for the hood is approximately 10 kW to 3000 kW. The velocity of gases flowing through the hood duct was measured using an Annubar®[1] averaging differential pressure element attached to a differential pressure transducer. The geometry of the duct system differed from that specified by the manufacturer, resulting in less flow straightening and flow development. Due to the difference, calibration fires were used to determine the flow coefficient for the differential pressure element.

Calibration fires were produced by a propane diffusion burner approximately 0.3 m by 0.3 m in size, providing fire heat release rates of approximately 35 kW and 50 kW. The propane burner heat release rates were calculated from the propane heat of combustion and the standard volume of propane provided to the burner as measured by a dry test flow meter corrected for temperature and pressure. For the oxygen consumption calculation of heat release from the propane burner, the value of E_{O_2} for propane is 12.78 MJ/(kg O_2) [7]. The combined standard uncertainty, composed of Type A and Type B uncertainties, in the base heat release measurements was 10 %. The expanded uncertainty in the base heat release measurements was 20 %, with a coverage factor of 2, which corresponds to a confidence interval of 95 % [8], [9].

During the experiments, the effects of wind and smoke escaping the sides of the hood increased the level of measurement uncertainty. The one open side of the test cell allowed prevailing winds to drive combustion products away from the hood. Fire resistant fabric side skirts reduced the loss of smoke, but wind conditions resulted in the loss of significant quantities of smoke in some experiments. For each HEAF fire experiment, additional uncertainty contributions due to wind and losses of combustion products were estimated using observations and video recordings.

Temperature and Heat Flux

One measure of the thermal environment during HEAF events and ensuing fires is the thermal heat flux imposed on materials surrounding the cabinets. There are various techniques available for measuring thermal heat flux, including water cooled transducers, slug calorimeters, directional flame thermometers (DFT), and plate thermometers (PT). The use of these transducers for measuring the heat fluxes in HEAF events was explored in an NRC funded project [10]. For the OECD program HEAF experiments, the choice of transducers was revisited.

The prime considerations for the experiments included a transducer that was sturdy and possessed a relatively short response time. One of the technologies frequently used in fire experiments is the water-cooled heat flux transducer (Schmidt-Boelter and Gardon Gauge types). There are two major drawbacks for their use in HEAF experiments, however. The first drawback is the presence of cooling water in the test cell, which presents logistical complications and safety hazards. The second drawback is related to the dynamic range of the

[1] Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

sensors. In order to capture the low heat fluxes from small ensuing fires to a reasonable level of uncertainty, a transducer with a measurement range from approximately 10 kW/m^2 to 200 kW/m^2 could be chosen, resulting in an expanded uncertainty of approximately 6 kW/m^2 (coverage factor of 2, 95 % confidence interval). A transducer of this range may be destroyed, however, by the fluxes resulting from impingement of plasma from the arcing portion of the experiment, which may be on the order of 1 MW/m^2. If a transducer with a measurement range high enough to survive the arcing is used, the heat flux measurement uncertainty would be too high for the ensuing fires.

Plate thermometers are robust sensors that can survive in hostile HEAF environments. A plate thermometer similar to that described in the literature [11], [12], and [13] was chosen for heat flux measurements in the OECD experiments due to its rugged construction, low cost, lack of cooling water, and emissivity and convective heat flux coefficients similar to power plant safety-related equipment.

The plate thermometer (PT) from the literature was modified for faster response and simpler manufacture. In order to decrease response time, the specified sheathed thermocouple was replaced by 0.51 mm diameter (24 AWG) Type-K thermocouple wires welded directly to the rear of an Inconel® 600 plate. The thickness of the mineral fiber blanket was increased to approximately 25.4 mm to decrease heat loss. A square plate of Inconel, approximately 100 mm by 100 mm in size, replaces the bent plate to reduce heat losses from the sides and simplify electrical isolation. Machine screws with ceramic washers allow for legs to be attached at the rear of the plate thermometer in order to simplify installation into cable trays and increase locational accuracy. The modified plate thermometer is shown in Figure 3 and Figure 4.

The incident heat flux on a plate thermometer can be calculated from a heat balance using the following relation, a rearrangement of Equation 18 from Ingason and Wickstrom [12]:

$$\dot{q}''_{\mathrm{inc}} = \sigma \cdot T_{\mathrm{PT}}^4 + \frac{(h_{\mathrm{PT}} + K_{\mathrm{cond}})(T_{\mathrm{PT}} - T_\infty)}{\varepsilon_{\mathrm{PT}}} + \frac{\rho_{\mathrm{ST}} \cdot C_{\mathrm{ST}} \cdot \delta \cdot \left(\frac{\Delta T_{\mathrm{PT}}}{\Delta t}\right)}{\varepsilon_{\mathrm{PT}}} \qquad (3)$$

Here $\dot{q}''_{\mathrm{inc}}$ is the incident heat flux, σ is the Stefan-Boltzmann Constant, 5.670×10^{-8} W/(m^2·K^4), T_{PT} is the temperature of the plate (K), h_{PT} is the convection heat transfer coefficient, 10 W/(m^2·K), K_{cond} is the conduction correction factor determined from NIST cone calorimeter data, 4 W/(m^2·K), T_∞ is the ambient temperature (K), $\varepsilon_{\mathrm{PT}}$ is the plate emissivity, 0.85 at 480 °C as rolled and oxidized and specified by the alloy manufacturer, ρ_{PT} is the alloy plate density, 8470 kg/m^3 from the alloy manufacturer, C_{ST} is the alloy plate heat capacity, 502 J/(kg·K) at 300 °C from the alloy manufacturer, δ is the alloy plate thickness, 0.79 mm, and Δt is the data acquisition time step of 0.2 s.

The modified PTs were heated in the cone calorimeter [14] to verify their performance and the fit of the simple thermal model in Equation (3). The plates were tested from 5 kW/m^2 to 75 kW/m^2 by heating from ambient temperature to steady state and then allowing them to cool. At a steady state flux of 75 kW/m^2 the calculated heat flux reached 63 % of the incident heat flux in approximately 0.7 s. The combined standard uncertainty in steady state heat flux measured by the plate thermometers, composed of Type A and Type B uncertainties, is 2.5 % at 75 kW/m^2. The expanded uncertainty in the steady state heat flux measurement is 5 % at 75 kW/m^2, with a coverage factor of 2 which corresponds to a confidence interval of 95 % [8].

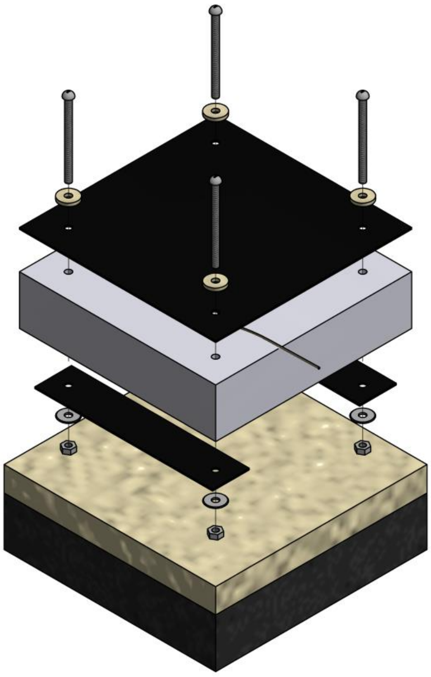


Figure 3 Exploded view of modified plate thermometer with cone calorimeter sample holder

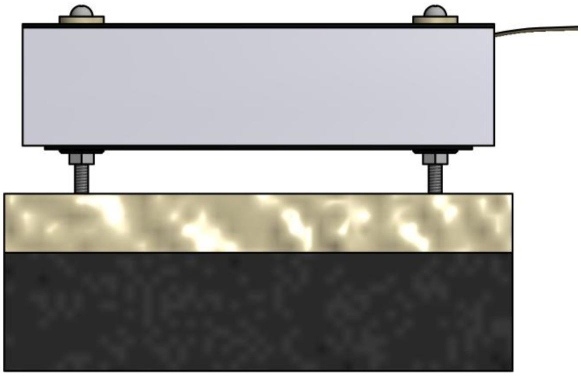


Figure 4 Elevation view of modified plate thermometer on cone calorimeter sample holder

The heating of plate TCs in the cone calorimeter was modeled in one dimension with the Fire Dynamics Simulator (FDS) [15] to verify the assumptions and property data. Agreement to within 1 % was found between the temperatures measured during exposure in the cone calorimeter and the FDS predicted temperatures. Data from heating the plate thermometer at 75 kW/m^2 in the cone calorimeter is included in the FDS validation library.

Sensor Wiring and Data Acquisition

Due to the voltages, currents, and electrical arcing that are present in and around the electrical equipment used in the HEAF experiments, electromagnetic interference (EMI) was present in the test facility. The electric and magnetic fields are capable of inducing voltages and currents in the sensor and data acquisition wiring. In order to reduce the effects of EMI, several strategies were employed in concert: shielding, isolation, signal conditioning, grounding, and electrical power conditioning. This multi-faceted approach greatly reduced or eliminated the effects of EMI on the measurement results.

A conceptual drawing of the sensors, instrumentation, and data acquisition is shown in Figure 5 and Figure 6. Figure 5 shows the wiring concept for a typical sensor, which includes plate thermometers and thermocouples. Figure 6 shows the wiring concept for the gas analyzers and differential pressure transducer for measuring hood flow rates.

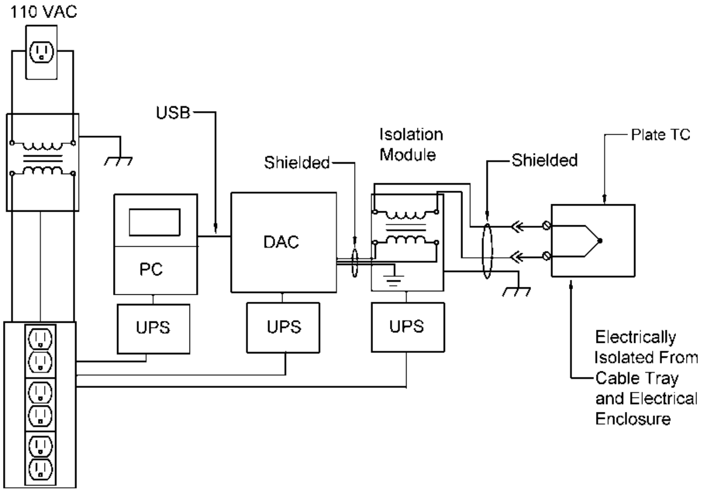


Figure 5 EMI resistant wiring concept for plate thermometer measurements

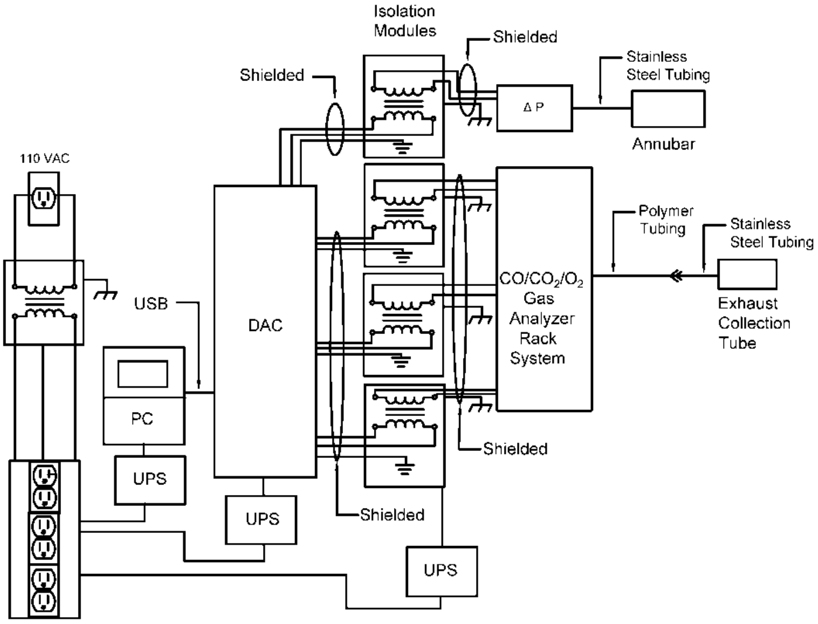


Figure 6 EMI resistant wiring concept for gas analysis and hood flow measurements

The sensor extension wiring is shielded, with the shield grounded near the sensor to earth ground. The sensor extension traveled through the test cell, via a route as far away from the current supply bus bars as practicable, through the back wall of the test cell, and to a signal conditioner and isolation transformer (isolation module). Each sensor channel had a dedicated isolation module. For thermocouple channels, the isolation modules also converted the low level mV signal produced by the thermocouple to a high level signal (0 VDC to + 5 VDC) linearized for a temperature range of – 100 °C to 1350 °C using a simulated ice junction.

Non-thermocouple sensors were served by isolation modules that converted the input signals to ± 1 VDC or ± 5 VDC output signals.

The output of each isolation module was connected to one of two data acquisition modules, housed in a separate enclosure, via a shielded cable that was grounded to earth ground. The high level signals from the isolation modules were sampled by the data acquisition system (DAC), with the results communicated to a laptop computer (PC) via a USB cable. Data were recorded by the data acquisition system at a rate of 5 Hz.

The main 115 VAC building power for the PC, data acquisition system, isolation modules, gas analyzers, and pressure transducer was supplied through signal conditioners, uninterruptible power supplies, and isolation transformers. The equipment chassis were grounded to earth. The heat release rate hood and duct support scaffolding were also grounded to earth. Grounding all of the equipment and cable shielding to the same earth ground prevented ground loops. The cable trays above the electrical enclosures were electrically isolated from the enclosure and hood and ungrounded. The enclosures were supplied with 3 phase power in a delta configuration, with the enclosure ungrounded.

RESULTS

Heat Release Rate

During the arcing phase of the HEAF experiments it was common for large quantities of rapidly generated combustion products to escape the measurement hood to the atmosphere and therefore avoid measurement. In order to measure heat release rate during the arcing phase, a larger hood would be needed to capture the combustion products, the size of which is impractical for a portable system. To measure larger fires, the exhaust mass flow rate would need to be increased, which would decrease the ability to resolve small fires, and increase measurement uncertainty. The purpose of the portable apparatus is to measure the HRR of the secondary phase of the HEAF event, i.e., the ensuing fire.

Oxygen consumption calorimetry for ordinary combustible materials such as flammable gases, flammable and combustible liquids, wood, and polymers utilizes a heat content of approximately 13.1 MJ/kg of oxygen consumed [5]. During the HEAF portion of the experiments, a significant quantity of copper and aluminum were oxidized. The heat release rate calculations do not take into account the difference in E_{O2} between oxidation of metals and the combustion of ordinary combustibles. During the HEAF portion of the experiments, the average heat release rate [MW] was estimated from the arc energy [MJ] divided by the arc duration (s) instead of oxygen consumption calorimetry.

The HEAF and ensuing fire from an experiment in a medium voltage cabinet are shown in Figure 7 and Figure 8. The nominal cabinet operating conditions were 7200 VAC and 24 kA with an arc of approximately 2554 ms in duration. The initial heat release from the cabinet due to the arc was not fully captured, but may be estimated as an average of approximately 28 MW from the arc energy expended during the arc. The heat release rate of the ensuing fire that occurred in the electrical enclosure following the HEAF event was recorded, with the primary fuel load consisting of the breaker housing. The maximum heat release rate of the ensuing fire was 165 kW. The expanded uncertainty in the heat release measurement is 25 %, with a coverage factor of 2, which corresponds to a confidence interval of 95 %.

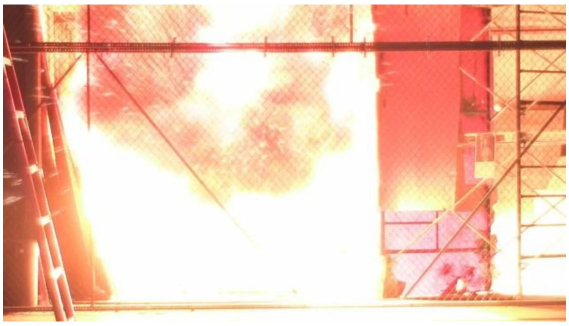


Figure 7 Medium voltage HEAF

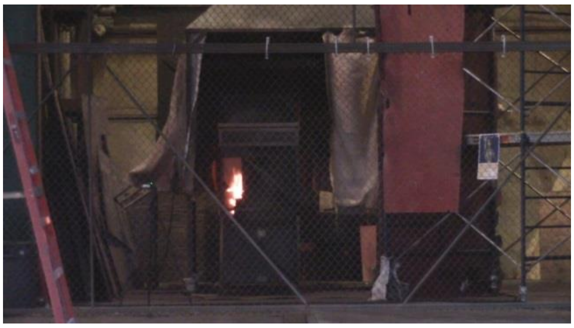


Figure 8 Ensuing fire

Temperature and Heat Flux

A low voltage HEAF in an enclosure with nominal operating conditions of 480 VAC and 50 kA with an arc of approximately 2115 ms in duration is shown in Figure 9 and Figure 10. The locations of the plate thermometers installed in the experiment are shown in Figure 1 and Figure 2. The temperatures reported by the thermocouples attached to the back of the nickel alloy plates of the modified plate thermometers are shown in Figure 11 and Figure 12.

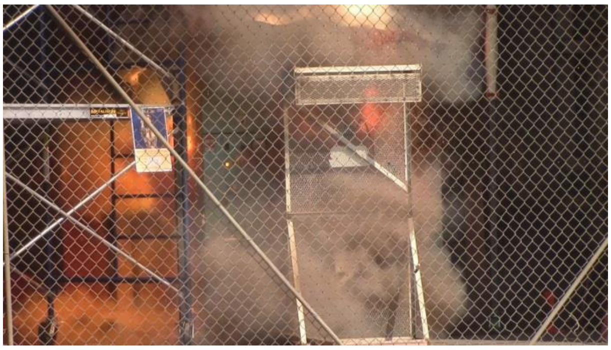
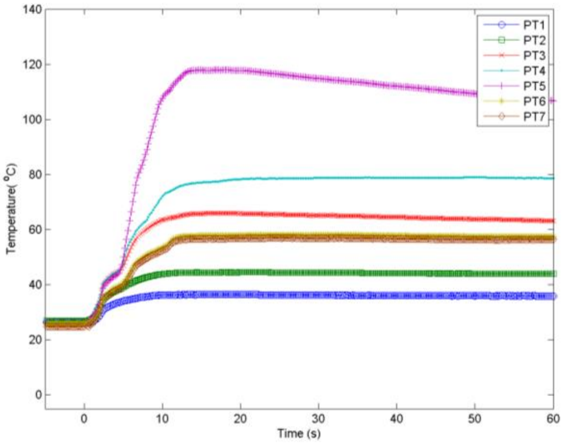


Figure 9 Low voltage HEAF; front of cabinet

Figure 10 Low voltage HEAF; top of cabinet; cable tray visible in upper right of photo

During some of the experiments, plate thermometers were directly impacted by plasma ejected from the cabinet. This contact resulted in abnormal thermocouple voltages and therefore to abnormal temperature change readings from the thermocouples. The resulting abnormal voltages, temperatures, and heat fluxes could be positive or negative. The data from plate TCs directly impacted by plasma could be used outside of the time where the arc was present by using the plate TC equations. An average heat flux during the arc can be calculated by treating the plate as a well-insulated, thermally-thin solid.

The heat flux histories of the plate thermometers in the low voltage experiment were calculated from the temperature data and are shown in Figure 13 and Figure 14. In this particular case, the plasma generated by the arc event did not cause significant abnormal voltages. The peak incident heat flux measured approximately 0.9 m (3 ft) from the cabinet at PT location 10 was 17 kW/m^2 during this experiment. The peak incident heat flux measured in the cable tray located approximately 0.3 m (1 ft) above the cabinet at PT location 5 was 72 kW/m^2 during this experiment.



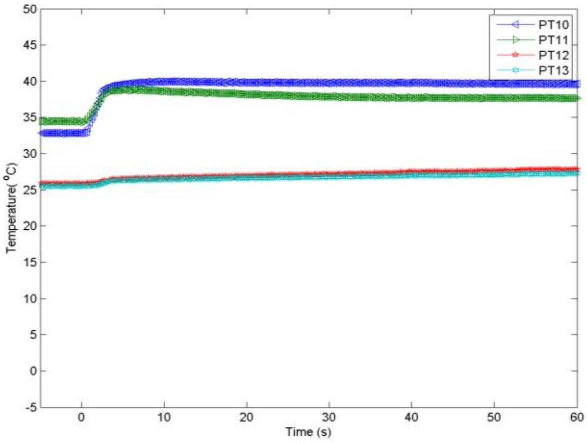
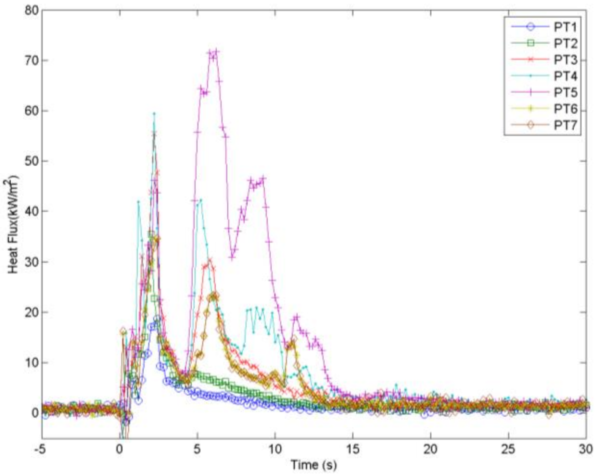


Figure 11 Cable tray plate thermometer temperatures, low voltage test. Temperature expanded uncertainty of ±3°C with coverage factor of 2

Figure 12 Vertical plate thermometer temperatures, low voltage test. Temperature expanded uncertainty of ±3°C with coverage factor of 2



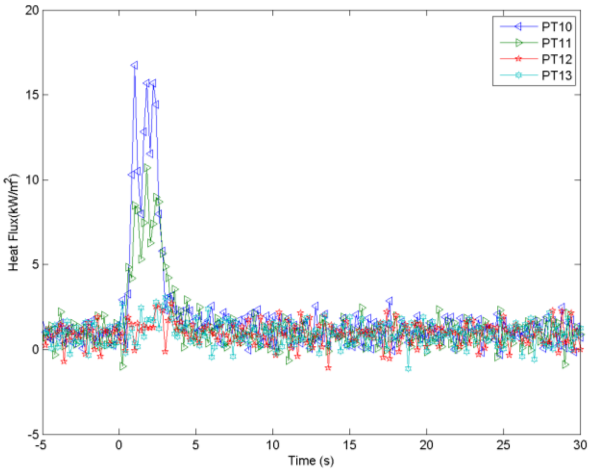


Figure 13 Cable tray PT heat flux, low voltage test; heat flux expanded uncertainty of ±4 kW/m^2 at 75 kW/m^2 with coverage factor of 2

Figure 14 Vertical PT heat flux, low voltage test; heat flux expanded uncertainty of ±4 kW/m^2 at 75 kW/m^2 with coverage factor of 2

The Fire Dynamics Simulator [15] was used to simulate the one dimensional heating of a plate thermometer (PT5 above) exposed to the heat flux history calculated from the plate thermometer measurement, Equation 3. The experimentally measured plate temperature and the corresponding FDS prediction agreed to within 2 %, which serves as verification of the method to calculate the heat flux from the measured plate temperature.

The test facility provided slug calorimeters for the measurement of the incident energy; that is, the total energy absorbed by thermally-thin targets at various locations around the enclosure. The incident energy was calculated from the temperature history according to standard methods [16]. The measurements from the slugs were also found to be adversely affected by direct impingement of plasma exiting the cabinets. The incident energy during the arc phase of the 480 V experiment was approximately 31 kJ/m^2 (0.75 cal/cm^2), measured at Slug 2.

CONCLUSIONS

The portable oxygen consumption calorimetry hood is effective for measuring the heat release rate of HEAF ensuing fires. As expected, HEAF arcing events produce too much effluent to be captured by the hood as designed. The average energy release rate during the arcing period, however, can be estimated from the electrically measured arc energy and arc time.

Plate TCs are an effective method for characterizing the thermal assault on NPP cable trays and equipment, and can serve as input boundary conditions for FDS modeling of target objects. Data during the arc event may need to be averaged over the time of the arc if plasma impingement on the plate TC causes abnormal signals.

ACKNOWLEDGEMENTS

The authors are grateful for the support of the participating OECD/NEA member countries, the OECD HEAF Project members, and the OECD/NEA. The authors also acknowledge the contributions of the other members of the NIST experimental team: Mr. Michael Selepak and Mr. John “Randy” Shields. Mr. Edward Hnetkovsky is acknowledged for fabrication of equipment and sensors. The authors are grateful to Dr. Kevin McGrattan of NIST for providing simulations of the plate TCs heated in the cone calorimeter and the HEAF experiment. Mr. Benjamin Lee of BSI is acknowledged for the calorimetry hood drawings included in this paper. Mr. David Stroup of NRC is gratefully acknowledged for serving as the NRC Project Manager for the NIST research effort. The authors are grateful to Mr. Mark Henry Salley of NRC for envisioning the cooperative relationship between NRC, OECD/NEA, and NIST for studying HEAF phenomena.

REFERENCES

[1] Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA), Committee on the Safety of Nuclear Installations (CSNI), *OECD FIRE Project - Topical Report No. 1, Analysis of High Energy Arcing Fault (HEAF) Fire Events*, NEA/CSNI/R(2013)6, Paris, France, June 2013, http://www.oecd-nea.org/nsd/docs/2013/csni-r2013-6.pdf.

[2] Electric Power Research Institute (EPRI) and United States Nuclear Regulatory Commission Office of Nuclear Research (NRC-RES), *Fire PRA Methodology for Nuclear Power Facilities,* EPRI/NRC-RES, Final Report, Volume 2: Detailed Methodology, EPRI 1011989, NUREG/CR-6850, Palo Alto, CA, and Rockville, MD, USA, September 2005, http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6850/.

[3] Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA), Committee on the Safety of Nuclear Installations (CSNI), Working Group IAGE (WGIAGE), *OECD NEA CSNI WGIAGE Task on High Energy Arcing Fault Events (HEAF)*, Task Report, NEA/CSNI/R(2015)10, Paris, France, 2015, https://www.oecd-nea.org/nsd/docs/2015/csni-r2015-10.pdf.

[4] McGrattan, K., S. Bareham, *Heat Release Rates of Electrical Enclosure Fires (HELEN-FIRE) - Draft Report for Comment,* NUREG/CR-7197, Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research, Division of Risk Analysis, Washington, DC, USA, 2015, http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr7197/.

[5] ASTM International, *Standard Practice for Full-Scale Oxygen Consumption Calorimetry Fire Tests*, ASTM Standard E2067-12, West Conshohocken, PA, USA, 2012, http://www.astm.org/Standards/E2067.htm.

[6] International Organization for Standardization, *BS ISO 5660-1:2015, Reaction to fire tests - Heat release, smoke production and mass loss rate - Part 1: Heat release rate (cone calorimeter method) and smoke production rate (dynamic measurement)*, Geneva, Switzerland, March 2015, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57957.

[7] DiNenno, P. J., Ed., *SFPE Handbook of Fire Protection Engineering*, 4th ed., Society of Fire Protection Engineers (SFPE), Bethesda, MD, USA, National Fire Protection Association (NFPA), Quincy, MA, USA, 2008, http://catalog.nfpa.org/SFPE-Handbook-of-Fire-Protection-Engineering-P13936.aspx?icid=D482.

[8] Taylor, B.N. and C. E. Kuyatt, *Guidelines for Evaluating and Expressing the Uncertainty of NIST Measurement Results*, NIST Technical Note 1297, National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, 1994, http://www.nist.gov/pml/pubs/tn1297/.

[9] Lafarge, T. and A. Possolo, "The NIST Uncertainty Machine", in: *NCLSI Measure J. Meas. Sci.*, to be published September 2015.

[10] Lopez, C., W. B. Wente, and V. G. Figueroa*, Evaluation of Select Heat and Pressure Measurement Gauges for Potential Use in the NRC/OECD High Energy Arc Fault (HEAF) Test Program*, Sandia National Laboratories (SNL), Albuquerque, NM, USA, 2014.

[11] Haggkvist, A., J. Sjostrom, and U. Wickstrom, "Using plate thermometer measurements to calculate incident heat radiation", *Journal of Fire Sciences*, Vol. 31, No. 2, 2013, pp. 166-177.

[12] Ingason, H. and Wickstrom, U., "Measuring incident radiant heat flux using the plate thermometer," *Fire Safety Journal*, Vol. 42, No. 2, 2007, pp. 161-166.

[13] Wickstrom, U., "The Plate Thermometer - A simple instrument for reaching harmonized resistance tests," *Fire Technology*, Vol. 30, No. 2, 1994, pp. 209-231.

[14] ASTM International, *Standard Test Method for Heat and Visible Smoke Release Rates for Materials and Products Using an Oxygen Consumption Calorimeter*, ASTM Standard E1354-15, West Conshohocken, PA, USA, 2015, http://www.astm.org/Standards/E1354.htm.

[15] McGrattan, K., et al., *Fire Dynamics Simulator, Technical Reference Guide*, Sixth Edition, NIST Special Publication 1018, Vol. 1: Mathematical Model; Vol. 2: Verification Guide; Vol. 3: Validation Guide; Vol. 4: Configuration Management Plan, National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, and VTT Technical Research Centre of Finland, Espoo, Finland, November 2013, http://firemodels.github.io/fds-smv/.

[16] ASTM International*, Standard Test Method for Determining the Arc Rating of Materials for Clothing*, ASTM Standard F1959 / F1959M-14, West Conshohocken, PA, USA, 2014, . http://www.astm.org/Standards/F1959.htm.

EVALUATION OF THE RANGE PERFORMANCE OF LASER SCANNERS USING NON-PLANAR TARGETS

Prem K. Rachakonda, Bala Muralikrishnan, Craig M. Shakarji,
Vincent D. Lee, Daniel S. Sawyer
Semiconductor and Dimensional Metrology Division,
National Institute of Standards and Technology,
Gaithersburg, MD, USA.

INTRODUCTION

The Dimensional Metrology Group (DMG) at the National Institute of Standards and Technology (NIST) is involved in the development of documentary standards for volumetric performance evaluation of laser scanners.

The proposed tests evaluate the performance of laser scanners by determining the measurement error between two derived points[§] at many positions in its work volume. Some of the proposed test positions are along the ranging direction of the laser scanner. Considerable work was done by the ASTM E57.02 committee on “Test methods”, however targets specified by the ASTM E2938 [1] standard are limited to planar targets.

This paper explores non-planar target artifacts such as spherical and trihedral targets, primarily to understand the influence of target geometry on ranging errors.

TARGET SELECTION

Flat planar targets are convenient to use in evaluating the relative range error. These targets are easy to fabricate or obtain commercially. They yield a measurand whose length value is dependent on its angle/orientation, processing method, density and distribution of data collected on the target.

A sphere’s derived point is its center and can be calculated with lower uncertainty by using a least-squares minimizing algorithm. For larger distances, larger diameter spheres are needed to capture enough data points on its surface. Since the sphericity (form) of the target sphere affects the determination of its center [2], obtaining commercially manufactured spheres of larger diameters and good sphericity is cost prohibitive. Spheres measured using laser scanners also suffer from the issue of having increased measurement noise towards the outer periphery of the sphere surface.

Contrast targets used by some laser scanner manufacturers employ proprietary methods to calculate the derived point on the target and hence are difficult to evaluate independently. Further, this derived-point calculation may not use the 3D point coordinates directly, but may use an indirect correspondence between the intensity data and the 3D coordinates.

In some proposed test positions for the volumetric evaluation, the targets may be located asymmetrically (not equidistant from the scanner). In such cases, the derived points calculated from the scans suffer from the problem of unequal range noise and uncertainty for all the four target geometries mentioned in this paper.

MEASUREMENT NOISE VS INCIDENCE ANGLE

A test was conducted to understand the effect of angle of incidence on the range noise of a laser scanner. This test consisted of mounting a flat aluminum plate on an adjustable stage and scanning multiple times at different angles.

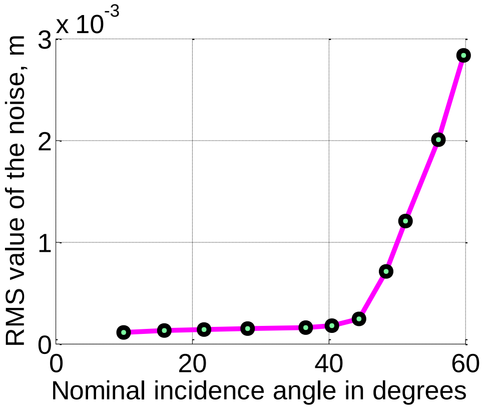


Figure 1. Noise vs incidence angle

[§] A derived point is a uniquely identifiable point on a target that is dependent on its geometry. Examples include sphere center, apex of a pyramid etc.

By fitting a plane to the scan data, the RMS (root-mean-square) values of the residuals (noise) were calculated. It was observed that the noise increases exponentially as the angle of incidence increases beyond 45º.

Figure 1 shows the results of this test. It should be noted that, the instrument manufacturer specifies a value of 50º as the angle beyond which the measurement signal deteriorates resulting in higher noise.

TESTS TO COMPARE RANGE USING TARGETS OF VARYING GEOMETRY

A series of four tests were performed to understand the effect of target geometry on the relative range error (E_{RR}). Each of the four tests varies in either the target geometry, or the procedure to calculate the reference/test length. The setup consists of two locations for the target on a sturdy tripod – a near position and a far position. The reference instrument (RI) was a laser tracker and the instrument under test (IUT) was a laser scanner. The four targets used in these tests were as follows:

a) Flat plane target
b) Trihedral target
c) Hollow sphere target
d) Integrating sphere target

For all targets except the integrating sphere target, the RI, IUT and the tripod positions were as illustrated in Figure 2. These three targets were tested simultaneously. For the fourth target (integrating sphere), the RI and IUT were on either side of the target as illustrated in Figure 3.

Of the two positions, the near position was at about 3 m away from IUT and the far position was about 8 m away from the near position, along the line joining IUT and the near position.

To reduce any errors due to the angular encoders, the RI and IUT need to be mounted on the same tripod in succession for taking the reference and IUT measurements. However, that was not the case in the setup described in Figure 2. This setup introduces an error of about 0.03 mm (1σ) in the reference length due to the angular encoder errors which was considerably smaller than the relative range errors.

In all the tests, four derived points were obtained - two at the near position and two at the far position. At the near position, the first derived point was obtained using the RI, and the second derived point was obtained using the IUT. The target was then moved to the far position and two more derived points were obtained similarly using the RI and IUT. Reasonable care was taken to make sure that the angle/orientation of the targets does not significantly change (with respect to the IUT). This was accomplished by marking the footprints of the tripod on the floor at both the positions and placing them back at approximately the same location during repeat measurements.

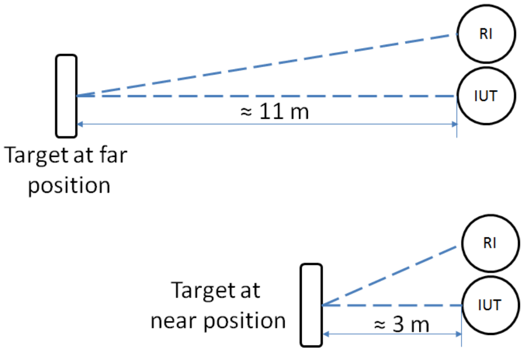


Figure 2. Location of RI, IUT and the two locations of 3 targets in Figure 4.

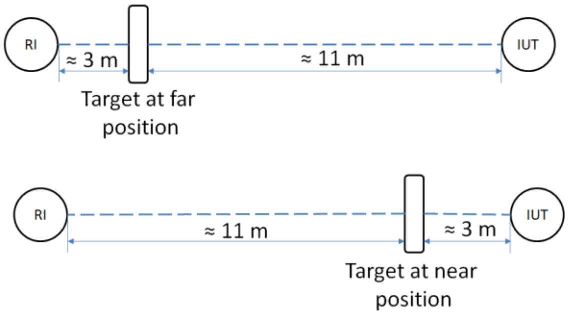


Figure 3. Location of RI, IUT and the two locations of the Integrating sphere target.

The reference length (L_{RI}) was the Euclidean distance between the derived points obtained using the RI at the near and the far positions. The test/IUT length (L_{IUT}) was the Euclidean distance between the derived points obtained using the IUT at the near and the far positions. The relative range error (E_{RR}) was calculated using equation 1.

$$E_{RR} = L_{IUT} - L_{RI} \qquad 1$$

In the next few sub-sections, the various target geometries are described and methods to obtain

L_{IUT} and L_{RI} are explained. These values were then used to calculate E_{RR}, using equation 1.

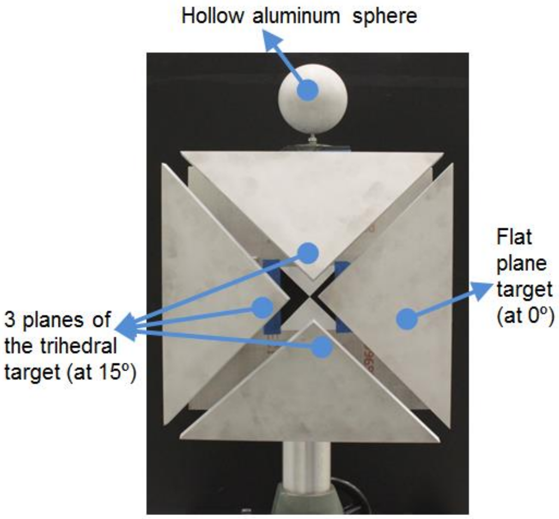

Hollow aluminum sphere
Flat plane target (at 0°)
3 planes of the trihedral target (at 15°)

Figure 4. Picture of the trihedral, flat and hollow aluminum sphere targets mounted on a tripod

Flat plane target:

The flat plane target was constructed from a triangular aluminum plate as depicted in Figure 4. Its surface was bead blasted to make its surface diffusely reflecting for the laser scanner. The derived point was the centroid of this plane. This target was mounted on to the tripod and placed at the near position and the far position successively and was measured using the RI and IUT to calculate the relative range error E_{RR}.

Calculating L_{RI}: To obtain the two derived points for the reference length using the RI, seven points were measured on the flat plate at both the positions (near and far) using the SMR (surface mounted retroreflector) walking method [2]. Three points were collected close to the vertices of the triangle, three points at the mid points of the sides and one point at the center of the triangular plate. The Euclidean distance between the two derived points (centroids) at the near and far positions will yield an L_{RI} value. A repeatability test was conducted to estimate the variation in the reference length in the ranging direction and the 1σ variation of 10 measurements was 0.165 mm.

Calculating L_{IUT}: The test length (L_{IUT}) was calculated by using the following procedure:

a) First the scan data was segmented to obtain the data corresponding to the flat plate.
b) Then the edge points were eliminated. This was performed by considering a cylindrical region whose axis passes through an initial centroid of the scan data and was along the ranging direction. The radius of this cylindrical region was empirically determined to exclude the edge points. All the points within this cylindrical region were considered for further processing.
c) A plane fit was performed on the data obtained in step #b) and the residuals were obtained. Points corresponding to the residuals exceeding two times the standard deviation (2σ) value were excluded from this data.
d) A centroid was calculated for the data obtained in step #c) and this was the derived point for the flat plane.
e) Another derived point was obtained at the far position and the Euclidean distance between the two derived points was the test length (L_{IUT}).

Note that this procedure for the flat plane target does not adhere to the procedure described in the ASTM E2938 [1] standard.

Trihedral target:

Three aluminum flat triangular plates similar to the flat plane target were used to form a trihedral target and are depicted in Figure 4. The derived point for this target was the intersection of the three planes. This target was first mounted on to the tripod. It was then measured using the RI and IUT while placed at the near position and then at the far position to calculate the relative range error E_{RR}. The three planes of the trihedral target were oriented in such a way that the incident angle of the laser beam from the IUT was ≈15°.

Calculating L_{RI}: To obtain the two derived points for the reference lengths using the RI, the three planes were measured using the method similar to that for the flat plate. Seven points were measured on each of the three surfaces of the target and three planes were fitted to these three sets of data. The intersection of these three planes was the derived point of the trihedral target. The Euclidean distance between the two derived points at the near and far positions will yield L_{RI}. A repeatability test was conducted to estimate the variation in the reference length in the ranging direction and the 1σ variation of 10 measurements was 10 μm.

Calculating L_{IUT}: To obtain the derived point using the IUT, the data on each of the three planes was processed using the steps a), b), and c) described for the flat-plane target. Three planes were then fit to these three sets of data and the intersection of these three planes was the derived point for the trihedral target. Similarly, the second derived point was calculated at the far position and the test length (L_{IUT}) was calculated.

Hollow spherical target:

A bead blasted hollow aluminum sphere (101.6 mm in diameter) was mounted on the tripod as depicted in Figure 4. The derived point for this target was the sphere center.

Calculating L_{RI}: The two derived points for the reference length were the two sphere centers calculated by using the SMR walking method [2]. A set of ≈15 points were measured on the sphere surfaces at both the positions using the RI. The sphere centers were then calculated by fitting a sphere using a constrained non-linear least squares algorithm. The Euclidean distance between the two sphere centers at the near and far positions will yield L_{RI}. A repeatability test was conducted to estimate the variation in the reference length in the ranging direction and the 1σ variation of 10 measurements was 0.010 mm.

Calculating L_{IUT}: The two derived points for calculating the test length (L_{IUT}) were obtained by first scanning the spheres at both the positions (near and far) using the IUT. The scan data was segmented to extract the sphere region and was then fitted using a constrained non-linear least squares algorithm.

Integrating sphere target:

A commercial sphere called the “Integrating sphere” was used in this test. This is a truncated sphere (100 mm in diameter) that has a pocket milled into the truncated portion of the sphere. Centered at the bottom of this pocket is a kinematic seat for a 1.5 in. diameter (38.1 mm) SMR/sphere. The concentricity of a 1.5 in. (38.1 mm) diameter sphere and the Integrating sphere, as measured by a coordinate measuring machine (CMM) was <10 µm. The derived point for this target was the sphere center.

Calculating L_{RI}: The two derived points for the reference lengths were an average of 20 points as measured by the RI using an SMR when it was seated in the integrating sphere’s kinematic seat. A set of 10 points were obtained from the RI before the IUT measurement scan and 10 points after the scan. A repeatability test was conducted to estimate the variation in the reference length in the ranging direction and the 1σ variation of 10 measurements was 0.005 mm.

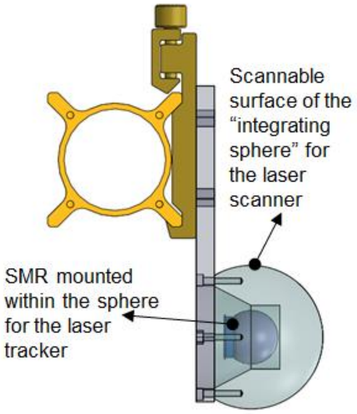

Scannable surface of the “integrating sphere” for the laser scanner
SMR mounted within the sphere for the laser tracker

Figure 5. Illustration of the top view of integrating sphere mounted for measurement by the IUT and RI

Calculating L_{IUT}: The two derived points for calculating the test length (L_{IUT}) were obtained by a process similar to that for the hollow sphere. The sphere was scanned at both the positions (near and far) using the IUT. The scan data was then segmented to extract the sphere region and the data was fitted using a constrained non-linear least squares algorithm.

RESULTS AND DISCUSSION

For each of the four targets, eight values of relative range error (E_{RR}) were obtained. Figure 6 shows a plot of the relative range errors for various target geometries and Table 1 shows the corresponding statistics for each target.

A few observations can be made from these results:

- The two spherical targets have the lowest variation (1σ) in the relative range error (E_{RR}) compared to the other targets.
- The flat plane target has the largest variation (1σ) of E_{RR}.
- The E_{RR} values for both the spheres were statistically similar.
- The trihedral target has the lowest absolute mean value of $E_{RR,}$ but has

slightly higher 1σ variation than the spheres.

- The flat plane target has the largest absolute mean value of E_{RR} apart from the largest 1σ variation of E_{RR}. An explanation for a possible reason for such a large bias will be provided later in this section.
- The flat plane targets measure shorter than their reference lengths, whereas the spherical targets measure longer than their reference lengths.

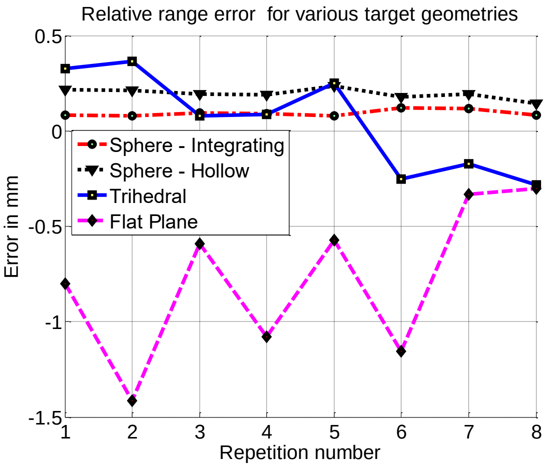


Figure 6. Plot showing the relative range errors for various geometries

Table 1. Statistics for the relative range error tests on four targets

Target type	Nom. length (L_{NOM})	1σ of L_{RI} (mm)	Mean of E_{RR} (mm)	1σ of E_{RR} (mm)
Sphere-I**	7.8 m	0.005	0.094	0.017
Sphere-H**	8.4 m	0.010	0.195	0.028
Trihedral	8.4 m	0.010	0.051	0.259
Flat plane	8.4 m	0.165	-0.781	0.403

Flat plane targets using the centroid as a derived point resulted in relative range errors that were larger compared to other targets used in these tests. The measurement of the derived-point to derived-point lengths for data from both the instruments relies on the target plates to be perfectly parallel.

For two perfectly parallel planes, if the centroids determined by RI and IUT are not identical, then the error is negligible as this error is not in the ranging/sensitive direction (cosine/second order error). However, if the planes are not parallel, an error in the centroid determination will result an error in the sensitive direction (first order error). This was exacerbated by the fact that the reference length was calculated based on a centroid determined by only seven points at each position.

As an example, consider two flat plane targets at the near position and the far position that are not parallel and are at 1° with respect to each other. Also consider that there is a 5 mm error in locating the centroid in the plane perpendicular to the sensitive direction. Such a setup will result in an error of 87 µm error in the relative range.

We plan to perform more tests using the flat plane target by making sure that the targets at the near and far positions are truly parallel and using alternative processing methods. The parallelism might be achieved by designing a kinematic mounting setup that uses a plane mirror and a laser for alignment.

One alternative processing method is to fit the data from the near and far locations using a parallel plane fitting algorithm [3] and calculating the distance between the fitted parallel planes. This method can still suffer from a first order effect with respect to the parallelism of the planes. Other methods to try include a bounding box method and the intersection of diagonals [1].

CONCLUSION

Four targets were tested for measuring relative range error of a laser scanner. Of these, one used a flat plane target. The flat plane target, where the centroid was the derived-point for the reference length results in larger relative range errors compared to the other three targets.

In contrast, spheres and trihedral targets have lower relative range errors and are less sensitive to their angle/orientation with respect to RI and IUT.

These tests indicate that the target geometry, alignment and the processing method affect the relative range error. More tests are planned (various lengths and processing methods) to understand the effect of target geometry on the relative range error.

** Sphere-H is the hollow sphere and Sphere-I is the integrating sphere

REFERENCES

[1] ASTM E2938 standard: "Test method to evaluate the relative-range measurement performance of 3D imaging systems in the medium range"

[2] Rachakonda, P., Muralikrishnan, B., Lee, V., Sawyer, D., Phillips, S., Palmateer, J., "A Method of Determining Sphere Center to Center Distance Using Laser Trackers For Evaluating Laser Scanners", Proceedings of the American Society for Precision Engineering, Annual Conference, Boston, Massachusetts, November 09-14, 2014.

[3] Shakarji, C., Srinivasan, V., "Theory and algorithms for weighted total least-squares fitting of lines, planes, and parallel planes to support tolerancing standards", Journal of Computing and Information Science in Engineering,13(3)

TARGETS FOR RELATIVE RANGE ERROR MEASUREMENT OF 3D IMAGING SYSTEMS

Prem Rachakonda[1], Bala Muralikrishnan[1], Meghan Shilling[1], Geraldine Cheok[2], Vincent Lee[1], Christopher Blackburn[1], Dennis Everett[1], Daniel Sawyer[1]

[1]Engineering Physics Division & [2]Intelligent Systems Division
National Institute of Standards and Technology,
Gaithersburg, MD, USA.

1 INTRODUCTION

The Dimensional Metrology Group (DMG) at the National Institute of Standards and Technology (NIST) is performing research to support the development of documentary standards within ASTM E57 [1] for the point-to-point performance evaluation of 3D imaging systems that use a spherical coordinate system.

The currently proposed tests call for the evaluation of point-to-point performance of these systems by determining the measurement error between two derived points* at a number of positions in the instrument's work volume. A part of the proposed standard involves measurements along the ranging/radial direction of the instrument and investigations were carried out at NIST to understand the suitability of various targets for this aspect of the standard. This paper will only discuss the variety of artifacts that were considered and investigated for use in these ranging test positions. The other aspects of the point-to-point tests are covered in another report [2].

2 OVERVIEW OF STANDARDS ACTIVITIES

The ASTM E57.02 sub-committee on "Test Methods" started work in 2007 to standardize test methods to evaluate the performance of 3D imaging systems. The first test that the sub-committee decided to develop was the relative range test because the ability to measure range was fundamental to these systems. The work concluded in 2013 and a relative range standard was published in 2015 (ASTM E2938 [3]).

In 2013, the sub-committee started to work on an expanded scope to evaluate the point-to-point performance of these instruments. The sub-committee meets every two weeks over a WebEx† teleconference to present the technical work and discuss the proposed standard.

The initial draft of this point-to-point performance standard has 12 two-face tests and 35 point-to-point tests, repeated three times. Two-face tests involve the measurement of a single stationary target using the front face and again using the back face of the instrument under test (IUT) [4].

* A derived point is a unique point obtained from a group of measured points on an artifact and is not a measured point. It is dependent on the artifact geometry. Examples include a sphere center obtained by fitting a sphere to points measured on the sphere's surface; the apex of a pyramid obtained by the intersection of three or more planes by measuring the planar surfaces of the pyramid.

† Disclaimer: Commercial equipment and materials may be identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Rachakonda, Prem; Muralikrishnan, Balasubramanian; Shilling, Katharine; Cheok, Geraldine; Lee, Vincent;
Blackburn, Christopher; Everett, Dennis; Sawyer, Daniel.
"Targets for Relative Range Error Measurement of 3D Imaging Systems."
Paper presented at The Coordinate Metrology Society Conference, Nashville, TN, Jul 25-Jul 29, 2016.

The distance between the derived points obtained from the front face and back face is itself the error; no reference length measurements are required for these tests.

Point-to-point tests involve measuring the distance between two targets using a reference instrument (RI), then with the IUT and comparing them. The draft standard on point-to-point performance includes point-to-point tests in both the radial and non-radial directions. Of these 35 tests, three tests are along the ranging/radial direction.

By the end of 2015, a test facility for implementing the point-to-point tests was established at NIST and in May 2016, a run-off meeting was held to allow manufacturers to evaluate all of the tests in the draft standard. Five manufacturers participated in this meeting, performed all the tests and provided feedback to improve the standard.

A significant topic that was debated prior to and during the run-off meeting was the choice of target geometry for the three ranging direction tests. The sub-committee agreed that a target with spherical geometry would be used for all two-face tests and all point-to-point length tests that are not along the radial direction. However, it was not clear if spheres would be suitable for long ranging/radial length tests. In this context, the DMG at NIST investigated various artifact geometries to determine their relative merits as targets for the ranging/radial length tests.

The next sections will discuss the targets that were considered and the objective criteria to evaluate each of them.

3 OVERVIEW OF RELATIVE RANGE TESTS

A relative range test is performed by placing the target at two positions (a near position and a far position), measuring the target at both positions with the IUT and the RI and calculating the relative range error. If L_{IUT} and L_{RI} are the distances between the targets as measured by the IUT and RI respectively, then the relative range error (E_{RR}) is given by: $E_{RR} = L_{IUT} - L_{RI}$. The RI in all the tests performed at NIST is a laser tracker and the IUT is a laser scanner, however the choice of instrument for RI is left to the user.

Depending on the design of the target, the relative range tests can be performed in one of two configurations. In the first configuration, both the RI and IUT are on the same side of the target (Figure 1) and in the second configuration, they are on the opposite side of the target (Figure 2). Alternative configurations were proposed and discussed by the sub-committee, but these two configurations offered lower uncertainties in obtaining the reference lengths.

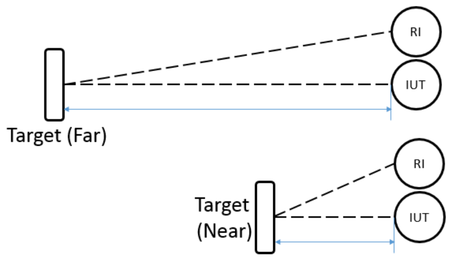


Figure 1: Relative range test with RI and IUT on the same side of the target.

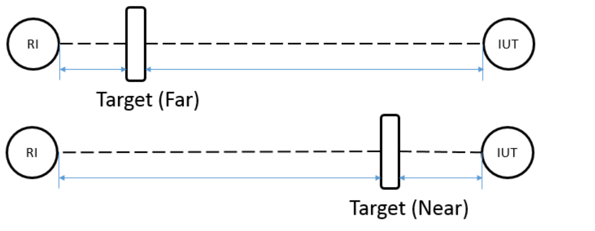


Figure 2: Relative range test with RI and IUT on either side of the target.

The choice of the configuration depends on the procedure to obtain the derived point using the RI. It should be noted that, the configuration in Figure 1 yields a slightly greater uncertainty in determining the reference lengths as the RI is not in-line with the target positions. In such a configuration, errors associated with the angular encoders increase the reference length uncertainty. Even though the configuration in Figure 2 offers lower uncertainty (than the first configuration), it results in higher uncertainty for shorter lengths and lower uncertainty for longer lengths. This may be problematic as the IUT will likely have tighter specifications for shorter lengths and wider specifications for longer lengths.

The published ASTM E2938 [3] standard mandates the use of plane targets. Since the work on this standard concluded in 2013, new targets started becoming commercially available that offer more efficient ways to realize these tests. The pros and cons of each of these targets will be discussed in the subsequent sections.

4 CHARACTERISTICS OF AN IDEAL TARGET

To objectively evaluate the benefits of various targets, some of the following characteristics were considered:

1. The IUT has to be able to measure the targets at all the test distances[‡] (1 m to 60 m), with respect to size and reflectivity and result in reliable data to calculate a derived point.
2. Measurement of the reference distance should be as simple/convenient as possible and practical in order to reduce measurement time.
3. The derived point needs to be obtained from dimensional data only (instead of intensity images etc.)
4. The RI and IUT have to measure the same point on the target so as to permit comparison of the measured lengths.
5. The target should be able to be aligned and mounted in a manner which minimizes the reference length uncertainty (U_{RL}) and results in U_{RL} that is a suitable fraction of the IUT specification limit.
6. The measurement procedure should limit the physical touching of the target or the mounting apparatus to prevent introduction of additional errors.
7. The target influences (such as geometry, surface finish, texture, color, lack of symmetry etc.) on the measurement should be as small as practically possible.
8. The procedure to obtain the derived point should be sufficiently repeatable over the entire testing range.
9. The target has to be relatively inexpensive to fabricate.

Five target types were considered for the purpose of evaluating the relative range of 3D imaging systems, namely a) Planes, b) Contrast targets, c) Spheres, d) Pyramids and e) Hybrid targets. They will be discussed in the subsequent sub-sections:

4.1 Planes

Planar targets have geometries that are simple and introduce insignificant geometry dependent errors that vary with range. The plane targets that are considered for use with laser scanners are metal

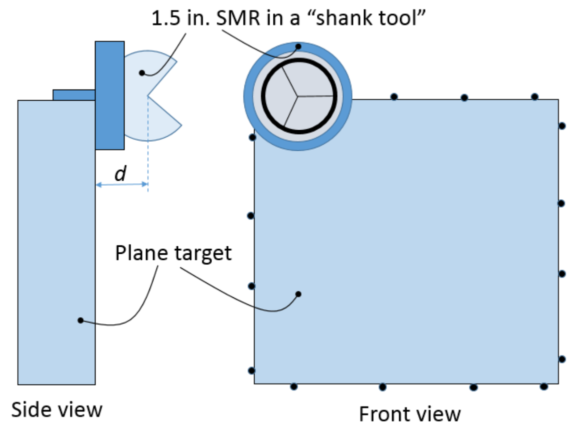


Figure 3: An illustration of the measurement process to obtain the derived point of a plane target using a reference instrument.

[‡] The proposed tests are for IUT with a maximum range of 150 m. However, the long range facility at NIST is 60 m long and the artifacts can be reliably tested only within 60 m range. The instrument range may go beyond 60 m (Typically 100 m to 300 m)

(usually aluminum) that have been vapor/media blasted, resulting in a lambertian surface with diffuse reflectivity. Such surfaces result in data that has relatively low noise (when compared to shiny or dark surfaces) and a return signal that is of uniform intensity over its entire surface. The target specifications (flatness, finish etc.) are simple enough for most machine shops to fabricate them with relative ease.

The ASTM E2938 [3] standard allows a variety of methods to calculate the reference and test lengths between two target positions. One method to obtain the derived point of a square plane target is to use a “shank tool”, a spherically mounted retroreflector (SMR) and a laser tracker as an RI. A “shank tool” is a special commercial mount for an SMR that allows it to be positioned over an edge of the target to measure points that are offset from the plane. The two planes at the edge need to be nearly orthogonal to each other for an effective use of the “shank tool”. The procedure to obtain the derived point is described below and is illustrated in Figure 3.

1. An SMR mounted on a “shank tool” in conjunction with a laser tracker is used to collect 4 sets of data on a plane target (one set per edge). Each set consists of four points resulting in a total of 16 points. More points can be recorded and processed if needed.
2. A 3D line is fitted to each set of points corresponding to each of the four offset edges yielding four 3D line equations.
3. Points corresponding to the four corners are calculated by intersecting the four pairs of two adjacent 3D lines. Because two 3D lines may not intersect at all, the point of intersection of two 3D lines is the point in space which is the closest point to both of the lines, determined in a least-squares sense.
4. The average of these four intersection points is the centroid of an offset surface from the plane target. The offset distance ‘*d’* is equal to the distance from the base of the “shank tool” to the center of the SMR mounted in it (as illustrated in Figure 3).
5. A plane is then fit to the 16 points obtained in step #1. This is a plane that is offset from the target surface by the same distance ‘*d’* towards the IUT.
6. Another plane is constructed that is parallel to the offset plane (obtained in step #5) and is at a nominal distance *‘d’* away from the IUT.
7. The centroid obtained in step #4 is then projected on to the plane constructed in step #6.
8. This projected point is the derived point for the plane target.

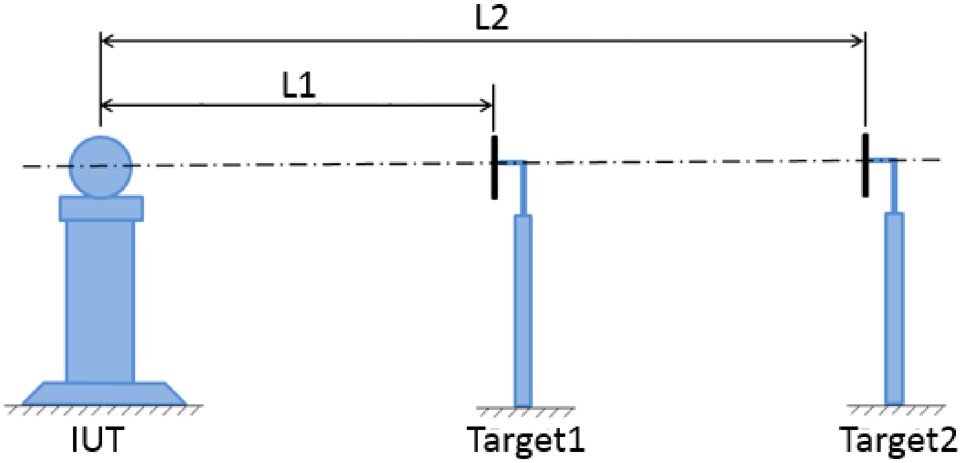


Figure 4: Relative range test with planes placed at two locations in-line with each other and the IUT (laser scanner)

To determine the centroid of the plane from the scan data, the following procedure is required by ASTM E2938 [3] standard.

1. Eliminate from the IUT data set all measured points that are part of the background, surroundings, and plane target supports.
2. Select measured points that will be used for the plane fit by omitting the measured points that are in the edge exclusion regions.
3. Fit a least-squares plane and calculate the standard deviations of the residuals.
4. Eliminate measured points on the plane targets for which the magnitude of the residuals is greater than twice the standard deviation of the residuals of the plane fit.
5. Determine the geometric center of the plane target using 2D or 3D methods.

To minimize the relative range errors, these targets need to be aligned perpendicular to the line joining the target positions and IUT (Figure 4). Any misalignment will result in Abbe errors that alter the relative range errors. For example, if the error in determining the geometric center of the plane (from IUT data) is 3 mm and if there is a 5° error in aligning the target with respect to the line joining the IUT and two target positions, this will result in 0.26 mm error in the ranging direction.

4.2 Spheres

Spheres are popular targets among users of 3D imaging systems (like laser scanners) as their geometry is the same in all the directions. This property is helpful when registering or aligning scans obtained from various positions. The derived point of a sphere target is its center and calculating a sphere center can be accomplished by a variety of established algorithms.

Three sphere targets were evaluated for relative range tests. They are a) Hollow - Painted plastic spheres, b) Hollow - Custom aluminum spheres, c) Special “integration spheres”. Each of these targets will be discussed in the following sections.

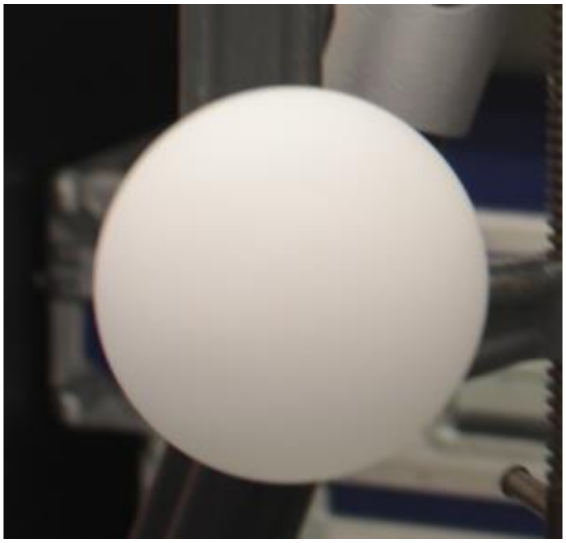


Figure 5: Hollow spheres – Painted plastic laser scanner sphere

4.2.1 Hollow – Painted plastic spheres

These are hollow plastic spheres that are typically painted with a white and diffuse coating and are mounted on a stem. These are commercially available from a variety of vendors. Due to the white paint used on these spheres, these spheres are visible to the 3D imaging systems from large distances.

These targets however are light, fragile and are not dimensionally stable. The form (sphericity[§]) on these spheres is also poor and is in the range of 0.3 mm to 2.0 mm, which results in an unacceptably large reference length uncertainty. These characteristics of the plastic spheres also make the determination of a reference length (with acceptable level of uncertainty) very challenging.

[§] In this publication, sphericity is defined as the smallest separation of two concentric spheres that contain all the points of the surface under consideration.

4.2.2 Hollow – Custom aluminum spheres

These are custom aluminum spheres (mounted on a stem) that are media blasted to provide a dull finish that is nearly lambertian. The form (sphericity) on these spheres is typically less than 0.02 mm on a 100 mm diameter sphere (by design). These are dimensionally stable artifacts that allow in-situ measurement using a laser tracker and an SMR to obtain the derived point (and thereby a reference length).

Though dimensionally stable, these spheres are less reflective than the painted spheres and do not scan as well at longer distances (compared to a similarly sized white painted sphere). Also, due to the fact that these are custom made spheres, they are more expensive and are not as readily available commercially as the painted spheres.

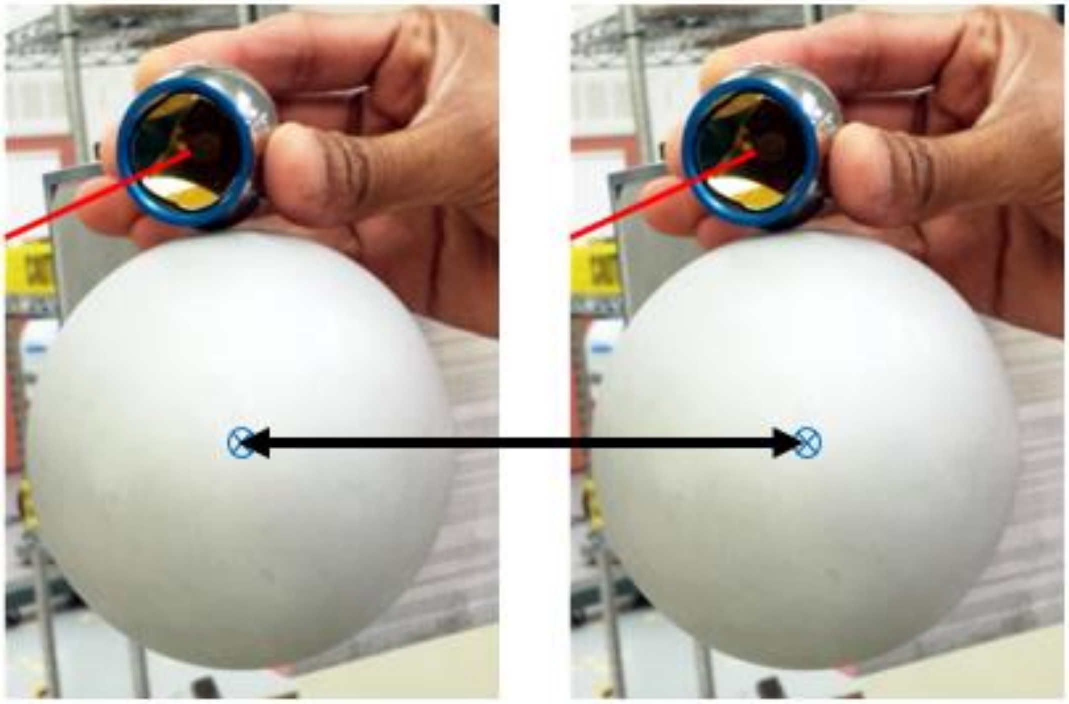


Figure 6: SMR walking method to obtain the reference length between two spheres.

To obtain the reference derived point of the sphere (sphere center), an SMR walking method [5] is used. Several points (typically more than 25) are obtained by probing the sphere surface using an SMR. The sphere center is determined by fitting these points using a non-linear least squares algorithm that constrains the radius of the sphere to its calibrated value (known a priori by measuring it on a touch probe CMM[**]). The second sphere is measured and the derived point is calculated using the same method. The distance between the two sphere centers is the reference distance for that particular test.

4.2.3 Integration spheres

These are commercial aluminum spheres that have a kinematic nest (with a magnetic preload) near their centers for a 1.5 in. diameter (38.1 mm) sphere or a 1.5 in. SMR. The kinematic nest is constructed in such a way that the center of a 1.5 in. diameter sphere (located in the kinematic nest) is concentric with the center of the outer sphere to within 0.01 mm. The form (sphericity) on these integration spheres is also within 0.01 mm and the outer surface has a near

[**] Coordinate measuring machine

lambertian finish. Custom modifications were done to add mounting holes on its outer periphery to mount it on a flat plate (as depicted on the right side in Figure 7).

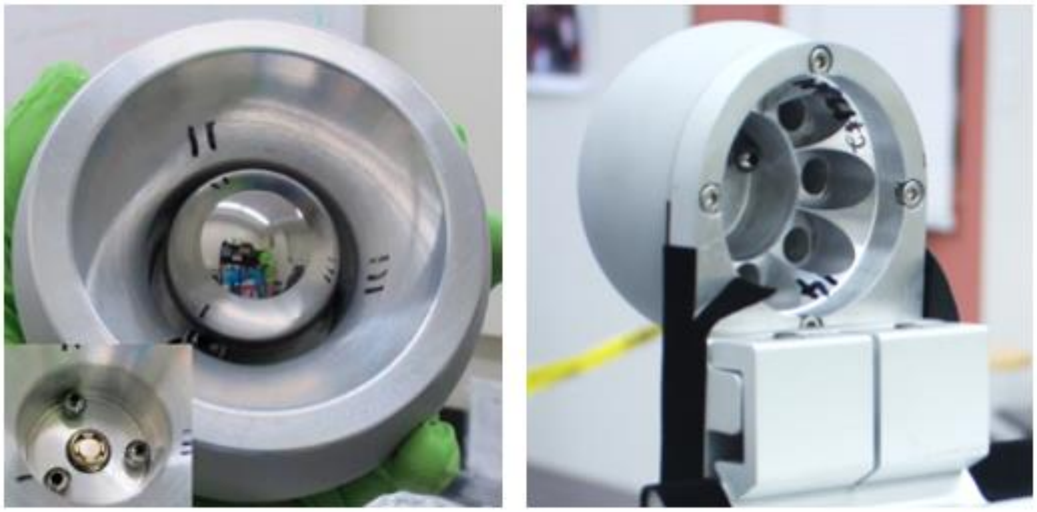


Figure 7: Two designs of a commercial “integration sphere”

To measure the reference distance between spheres at two locations, a single point measurement using a reference instrument is sufficient at each position. This process does not involve any touching of the target and minimizes any mounting related errors. This design allows the possibility of automating the reference length measurement and also techniques that could lower the reference length uncertainty [2].

4.2.4 Point cloud data considerations for spheres

Spheres, although suitable for the reasons discussed in the previous sections, have a few shortcomings with respect to data quality and reliability of the derived point obtained from such data. Some of these are discussed in the next few sub-sections.

4.2.4.1 Coverage

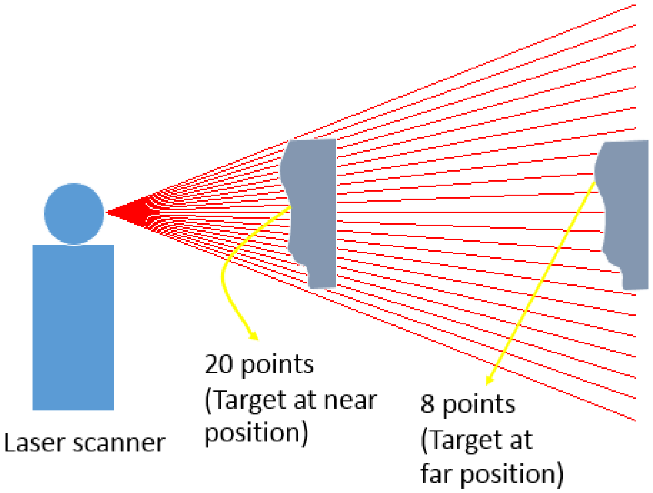


Figure 8: Point density variation from near to far position

For a given instrument setting, the number of points on a target that is farther from the IUT is less than that for a target that is closer to the IUT (as illustrated in Figure 8). For a sphere target, this issue is exacerbated by the fact that the return intensity is not the same from all the locations on its surface. Return beam corresponding to lower return signal intensity may not register with the instrument, resulting in missing points from a sphere’s outer periphery (compared with data from the sphere’s surface at the center). This reduces the “coverage area” of the scan data on a sphere at the farther location, compared with that at the nearer location (as illustrated in Figure 9). This in turn increases the error when calculating the center of the sphere using a non-linear least-squares fitting algorithm.

4.2.4.2 Squishing and Flaring of spheres

For some instruments, the quality of the scan data from the sphere surface varies over its surface from its center to the outer periphery. There are a number of hypotheses as to why this effect is observed: varying slope, beam width, multi-path effects due to the mounting apparatus or a variety of other instrument related error sources. Because of this, when the data from such targets is fit to a sphere using a non-linear least-squares algorithm without constraining the radius, the resulting radius (R_{UNC}) is different from its calibrated radius (R_{CAL}). As a result, the spheres may appear "squished" ($R_{UNC} < R_{CAL}$) or flared ($R_{UNC} > R_{CAL}$).

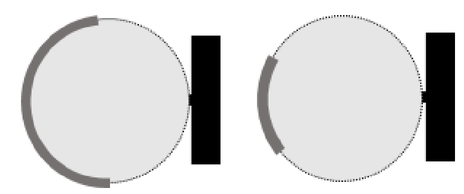


Figure 9: Coverage on a sphere at the near location (left) and at a farther location (right).

When the center of the sphere is determined using a constrained radius fit (as would be done to find the center to center distance for IUT evaluation), that center will be shifted towards or away from the IUT due to the squishing/flaring of the measured points, resulting in an apparent ranging error.

In most cases, the sphere appears to be "squished", rather than "flared". Also, in practice, this affect appears to be more prominent when using phase-based laser scanners than pulse-based laser scanners.

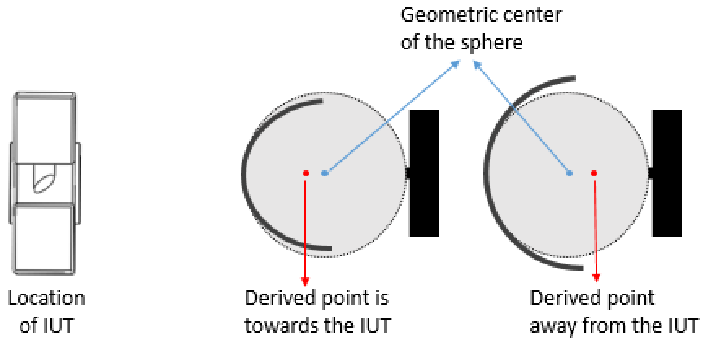


Figure 10: "Squishing" effect (left) and "Flaring" effect (right).

4.2.5 Contrast targets

Contrast targets are popular among the surveying community (depicted in Figure 11). One type of contrast target has planar targets mounted on truncated 1.5 in. (38.1 mm) diameter spheres in such a manner that the center of the truncated sphere lies on the front surface of the target. This center is designed to nearly coincide with the intersection point of the pattern shown in Figure 11.

The truncated sphere allows the contrast target to be mounted on magnetically preloaded kinematic nests. To determine the relative range error, the distance between kinematic nests (at two positions) is first measured using a laser tracker using a 1.5 in. SMR. The SMR is removed and a contrast target is placed in the same nests (one at a time) and scanned using a 3D imaging system [4]. Proprietary algorithms (that use both image intensity and dimensional data) are then used to obtain the derived points of each of the targets and thereby the distance between the two positions using the 3D imaging system.

Since the calculation of the derived point for a contrast target uses a combination of image intensity data and dimensional data, its accuracy and precision is dependent on a variety of factors such as contrast difference, orientation of the target etc. These issues make contrast targets less preferable for use in relative range tests for evaluating the dimensional measurement performance of 3D imaging systems.

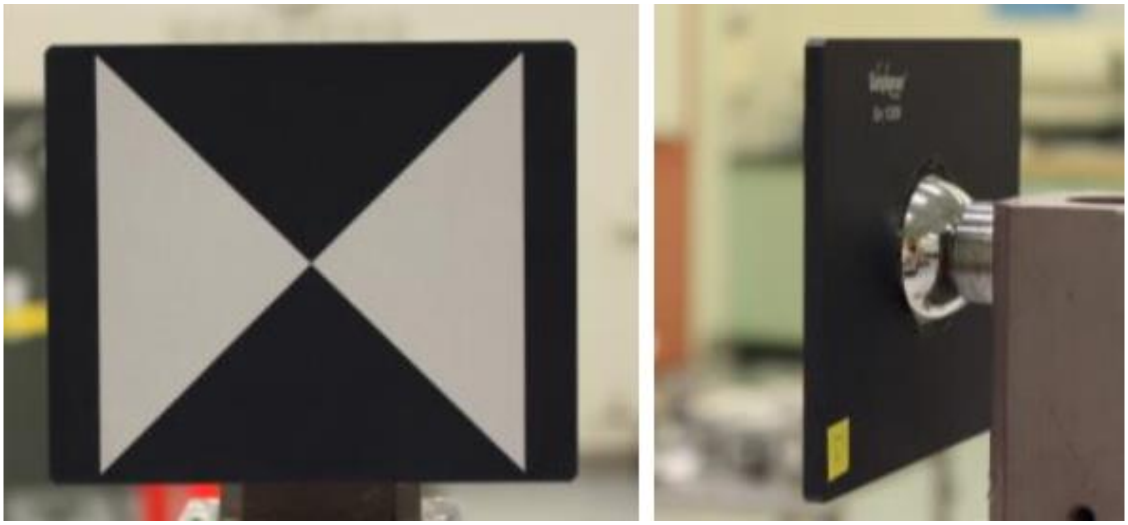


Figure 11: Contrast target front side (on the left) and back side with the truncated sphere mount (on the right)

4.2.6 Pyramid or Polyhedral targets

Pyramid or polyhedral targets attempt to address the shortcomings of the planar and spherical targets. These targets have three or more planes. The derived point of such targets is the apex, which is the intersection of the planes of the target. In case of a trihedral target (triangular pyramid), the intersection of the three planes is unique and is the derived point. In case of a target with more than three planes (e.g. square pyramid), the derived point is the intersection point of the four planes in a least-squares sense.

For a pyramid, the slant angle is the angle that each plane makes with the base of the pyramid (as illustrated in Figure 14). This slant angle is chosen so as to maximize the return signal intensity to the IUT while minimizing the errors associated with determining the intersection point of the planes.

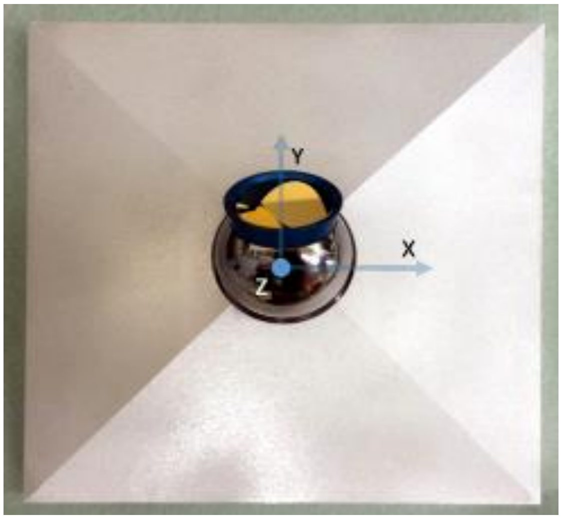


Figure 12: NIST tetrahedral target

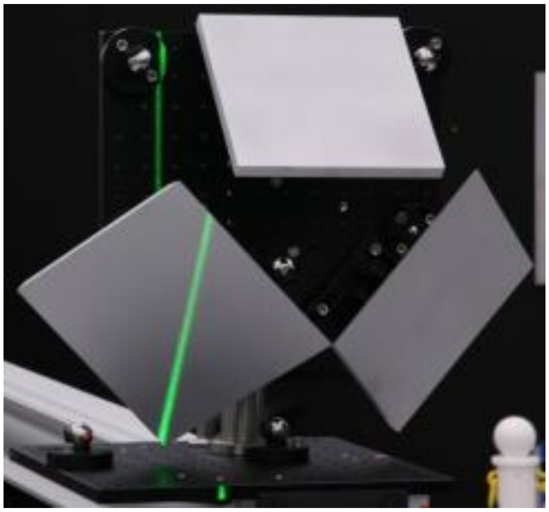


Figure 13: NRC trihedral target [6]

Polyhedral targets constructed with planes at shallow slant angles, say 1°, will not produce a sufficiently repeatable apex coordinate because of the noise in the data from the IUT. Small changes in the location and direction of the normal vector to the best fit planes (to the noisy data) create relatively large changes in the location of the apex. Polyhedral targets constructed with planes at a steep slant angle, say 75°, will also not produce a sufficiently repeatable apex coordinate. This is because of the fewer number of data points acquired on the plane and the fact that these points have higher noise levels due to the steep incidence angle of the laser beam with the plane.

Simulations were performed to understand the effect of the slant angle of a pyramid target on the repeatability of its apex. These simulations indicated that pyramid targets with a slant angles between 10° and 30° yield a sufficiently repeatable derived point (apex) when measured with laser scanner systems.

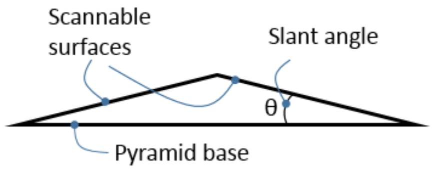


Figure 14: Slant angle of a pyramid artifact.

Determining the derived point using a laser tracker depends on the design of the target. If the target is designed as shown in Figure 12, where the SMR center is designed to be coincident with the apex, a single point measurement is sufficient to determine the target's derived point. For the design depicted in Figure 13, the SMR walking method may be used to manually probe each plane to determine the apex [6,7]. Another method to get the derived point for the same design in Figure 13 is to use three 1.5 in. (38.1 mm) diameter spheres mounted rigidly in kinematic nests on the plate holding the target. The apex of these planes is determined with respect to a coordinate system established by the centers of the three spheres and is calibrated on a CMM. During the relative ranging test, the RI is used along with a 1.5 in. SMR to calculate the apex (using the CMM data) with respect to the locations of the SMR centers located in these three kinematic nests.

The derived point from IUT data is calculated by extracting the data corresponding to each plane of the target, fitting a plane to each data set and intersecting them. The data set for each plane is obtained by excluding the edge points, either manually or by using an automated method.

The pyramid targets have some shortcomings when compared with other targets. The process of extracting a derived point from a pyramid target requires more steps than for other targets. Also, for the target depicted in Figure 12, the SMR needs to be concealed during a scan to avoid any specular reflections from the target.

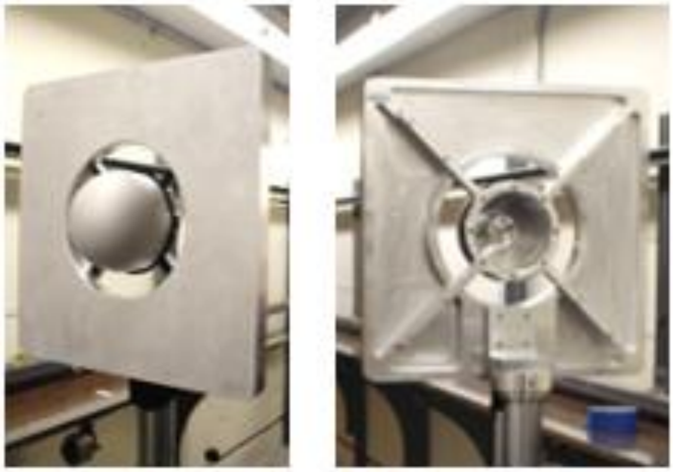


Figure 15: NIST Plate-sphere target

4.2.7 Hybrid targets

Hybrid targets, such as the Plate-sphere target designed at NIST (depicted in Figure 15), leverage the benefits of the geometries of both the sphere and a plane. A plane suffers from the lack of a unique derived point, but can be measured at large distances. A sphere suffers from the fact that its geometry introduces a high variability in determining the radial distance from the scanner to its center. A hybrid target like the NIST Plate-sphere target combines both these geometries to overcome and complement individual target inadequacies

The NIST Plate-sphere target uses a plate target and a 200 mm diameter integration sphere that has a 1.5 in. SMR mounted in its kinematic nest. The derived point for this target is obtained by using a laser tracker and the SMR located inside the integration sphere.

For this target, the 3D imaging system (IUT) and the laser tracker (RI) are placed on opposite sides of the target (as illustrated in Figure 2). The laser tracker measures the sphere center from one side and the laser scanner measures the derived point from the other.

The derived point using the laser scanner is determined using the following series of steps:

1. The sphere and the plane data are individually extracted from the scan data.
2. A least-squares plane is fit to the data corresponding to the plane.
3. A sphere is fit to the data corresponding to the sphere using a non-linear least squares algorithm that constrains the radius of the sphere to its calibrated value (known a proiri).
4. The sphere center is then projected on to the least-squares plane in a direction that is normal to the fitted plane.
5. This projected point is the derived point of this plate-sphere target.

This procedure to obtain the derived point overcomes the issue of high variability of a sphere center in the ranging direction and high variability of the centroid of a plane in the non-ranging directions. It also reduces the need to accurately align the target perpendicular to the laser beam.

One of the drawbacks of the Plate-sphere target is that the sphere occupies a sizeable portion of the center of the plate. When the target is close to the IUT, the data from the plane involves exercising the angular axes and also is not along the line joining the IUT and the RI. Another drawback is that this target is relatively expensive to fabricate.

4.2.8 Alternative designs

To overcome some of the shortcomings of the targets, two more designs are under consideration and are described below:

1. A Plate-sphere artifact with three or more spheres on the outer periphery of the plate to act as a fiduciary instead of a sphere at the center.
2. A Pyramid artifact similar to the one depicted in Figure 12, but designed in such a way that the SMR is accessible from the back of the pyramid.

5 SUMMARY

A variety of targets for use in relative ranging tests were designed and/or procured by DMG at NIST and evaluated. Each target was evaluated objectively based on a variety of desired characteristics, their relative merits and practicality. Each target offers distinctive advantages as well as a few disadvantages for this activity. More work is planned at NIST to improve on the existing designs to evaluate targets for relative ranging.

6 ACKNOWLEDGEMENTS

The authors would like to thank Mr. Luc Cournoyer of the National Research Council (NRC), Ottawa, Canada for his valuable feedback and suggestions that went into this work.

7 REFERENCES

[1] ASTM E57.02 – “Test Methods”, WK 43218: New Test Methods for Evaluating the Performance of Medium-range, Spherical Coordinate 3-D Imaging Systems for Point-to-Point Distance Measurements.

[2] Muralikrishnan, B., Rachakonda, P., Shilling, M., Lee, V., Blackburn, C., Sawyer, D., Cheok, G., Cournoyer, L., Report on the May 2016 ASTM E57.02 instrument runoff at NIST, Part 2 NIST realization of test procedures and measurement uncertainties, to be published as a NIST internal report.

[3] ASTM E2938 standard: “Test method to evaluate the relative-range measurement performance of 3D imaging systems in the medium range”

[4] Ferrucci, M., Muralikrishnan, B., Sawyer, D., Phillips, S., Petrov, P., Yakovlev, Y., Astrelin, A., Milligan, S., Palmateer, J., “Evaluation of a laser scanner for large volume coordinate metrology: A comparison of results before and after factory calibration", Measurement Science And Technology, September 2014.

[5] Rachakonda, P., Muralikrishnan, B., Lee, V., Sawyer, D., Phillips, S., Palmateer, J., “A Method of Determining Sphere Center to Center Distance Using Laser Trackers For Evaluating Laser Scanners”, Proceedings of the American Society for Precision Engineering, Annual Conference, Boston, Massachusetts, November 09-14, 2014.

[6] MacKinnon, D., Cournoyer, L., Beraldin, J., “Single-plane versus three-plane methods for relative range error evaluation of medium-range 3D imaging systems”, Proc. SPIE 9528, Videometrics, Range Imaging, and Applications XIII, 95280R (June 21, 2015)

[7] Rachakonda, P., Muralikrishnan, B., Shakarji, C., Lee, V., Sawyer, D., “Evaluation of the Range Performance of Laser Scanners using Non-Planar Targets”, Proceedings of the American Society for Precision Engineering, Annual Conference, Austin, Texas, November 01-06, 2015.

On The Feasibility of Performing Line Scale Measurements on a High Accuracy Coordinate Measuring Machine

W. Ren, R. Sundahl, T. Doiron
Engineering Physics Division
National Institute of Standards and Technology,
Gaithersburg, MD 20878

1. Introduction

1.1 History of NIST Line Scale Interferometer (LSI)

The linear distance between rules is a fundamental length measurement of vital importance in many scientific and industrial operations. From encoded scales to photo lithographic grids, linear rules are used as check standards and must be calibrated and traceable to the international standard of length. In 1958, the National Institute of Standards and Technology (NIST), then known as the National Bureau of Standards (NBS), developed an early design of an interferometric line scale comparator [1]. By 1981, the instrument was modernized and automated, and consisted of a scanning electro-optical line detector, a high precision one-axis motion system, and a high accuracy heterodyne interferometer for determining the displacement of the test artifact beneath the line detector [2].

1.2 Requirement changes for LSI measurement

Over the years, there has been a trend away from line standards as our calibration income chart in Fig. 1 shows. In recent years, we have calibrated only a few scales from industry; our largest customer for LSI measurements has been the NIST Dimensional Metrology Group itself. The LSI machine is very old and difficult to maintain. The expenses for upgrades to the machine are not feasible given the income and lack of industrial customers. This paper describes recent work in transitioning line scale measurements from this old LSI machine to a vision probe equipped Moore-M48 Coordinate Measuring Machine[1] (CMM) based platform. The clear advantage of such a transition is that we can employ a single CMM for multiple calibrations including line scales, thereby keeping our maintenance and operational costs to a minimum.

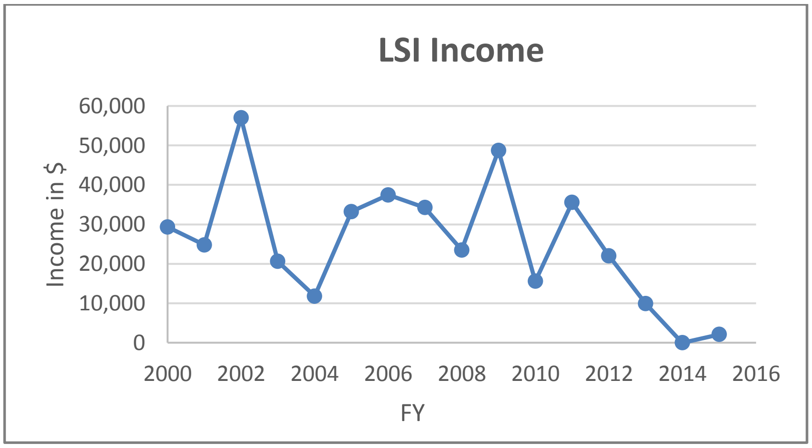


Fig. 1 NIST LSI calibration income

Ren, Wei; Sundahl, Roy; Doiron, Theodore.
"On The Feasibility of Performing Line Scale Measurements on a High Accuracy Coordinate Measuring Machine."
Paper presented at the NCSLI 2016 Workshop & Symposium Exhibition, Saint Paul, MN, Jul 24-Jul 28, 2016.

2. New NIST LSI System

2.1 CMM stage

The new NIST LSI system (Fig. 2) uses a Moore M-48 CMM as a precision stage to move the line standard under a video microscope. The CMM structure consists of a heavy cast iron, jig-grinder base. The machine rests directly on the floor of an underground laboratory. The extremely stable floor makes the vibration effect during image acquisition negligible. The X-axis table and the Y-axis cross-carriage motions are carried out by high precision lead screws immersed in oil baths and are guided by precision double “V” roller ways [3]. These motions are pulled against the thrust faces of the lead screws by constant force springs, reducing backlash. A flat granite surface plate is seated on the machine table which helps transform complex table motion errors into rigid body motion errors which are then mapped out. When the M48 is used as the LSI, we have an additional external laser system, where the vacuum wavelength is calibrated at NIST with a fractional expanded uncertainty of 5 x 10^{-9}, to record the table X-axis displacement, which makes the residual machine motion errors ignorable.

2.2 External laser system

Our external laser system includes a laser head sitting on a tripod on the floor capturing the table X-axis motion, an interferometer cube sitting on the M48 X-axis table, and a retro-reflector mounted behind and under the objective lens (Fig. 3). We mount the retro-reflector as close as possible to the focal point in order to accurately locate the position of the camera each time an image is acquired. Laser readings are influenced by the index of refraction of the air along the laser path; we monitor the temperature, barometric pressure and humidity along this path during image acquisition. We then correct the refractive index of air using a modified version of Edlén Equation.

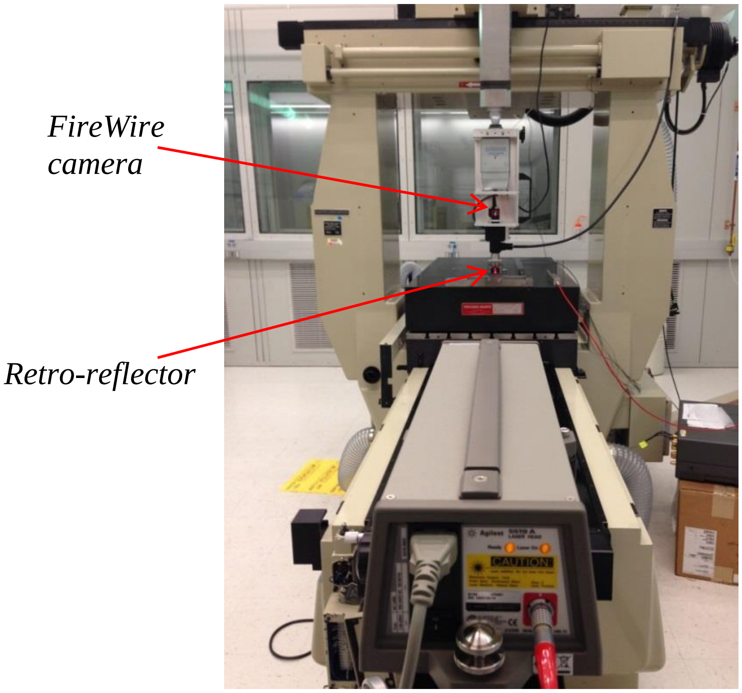


Fig. 2 New NIST LSI system on Moore M-48 CMM

2.3 Camera and Microscope

Our microscope system (Fig. 3) includes an industrial FireWire[1] camera, a white light LED illumination system, and a 50X objective lens. The system is mounted on the Z-axis ram of the CMM. The line images acquired by the camera under different lighting and different exposure times were tested to achieve the best quality image. For each line image, we use a LabView[1] advanced edge detection algorithm that uses a kernel operator to compute the edge strength to find the center of the line [4]. The kernel operator is a local approximation of a Fourier transform of the first derivative [4]. The algorithm also has the option to provide subpixel offset from the whole pixel location to find a better estimate of the edge location.

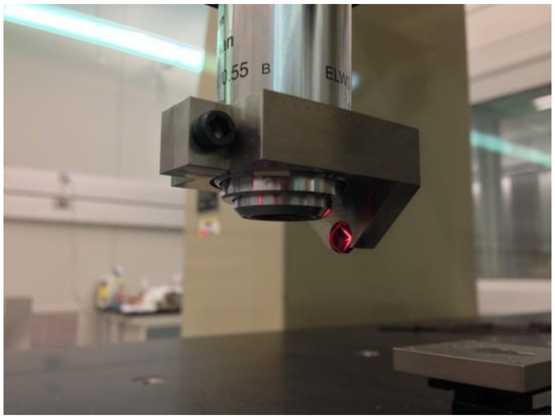


Fig. 3 A retro-reflector mounted on the objective lens

2.4 Software

A LabView program controls the operation of the LSI system. The program communicates with the CMM controller through an Ethernet connection to command the machine move to specific positions, acquires the image with the FireWire interface at each position, analyzes the image, computes the line position at each field of view, and saves the measurement data to a file. The program also records the laser readings during image acquisition and records temperature, barometric pressure, and humidity from individual instruments via USB ports after each image acquisition.

3. System Setup and Measurement Process

3.1 System alignment

Alignment of the artifact, laser and optics along the machine axis of motion is a critical aspect of LSI measurement [5]. The Z-axis of the camera must be aligned perpendicular to the XY plane. The laser beam must also be aligned with the X-axis table motion.

[1] Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

Finally, the line scale artifact must be aligned with the laser. It should be noted that a cosine error will be introduced if the laser beam is not aligned with the artifact to be measured. There are four steps to align the laser beam with the measurement artifact.

First, we align the laser head with the X-axis table motion using a retro-reflector mounted at the far end of the table. By moving the table back and forth along the X-axis, the laser should receive the return beam signal from the retro-reflector well centered with an X-Y shift of less than 0.5 mm. Second, we position the interferometer with a plain mirror sitting on the table and move the table back and forth along the X-axis to align the return beam with the laser detector. This laser serves as the reference beam in our LSI system. Third, we adjust the height of the retro-reflector, which is mounted on the back of the objective lens to align with the interferometer. The two return beams should overlap and be detected by the laser. When the CMM table moves, the distance between the interferometer and the retro-reflector reflects the position close behind and above the focal point of the microscope objective. Finally, we find the center of laser beam, which we call the measurement line. (Fig. 4) We locate the measurement line by searching for the laser signal boundary at the near and far ends and find the centers. We then align the scale along the measurement line by adjusting the position of the scale to keep both ends of the scale in focus.

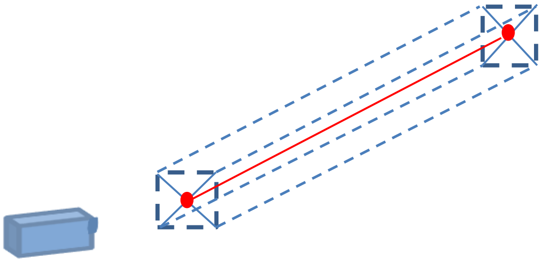


Fig. 4 Measurement line alignment

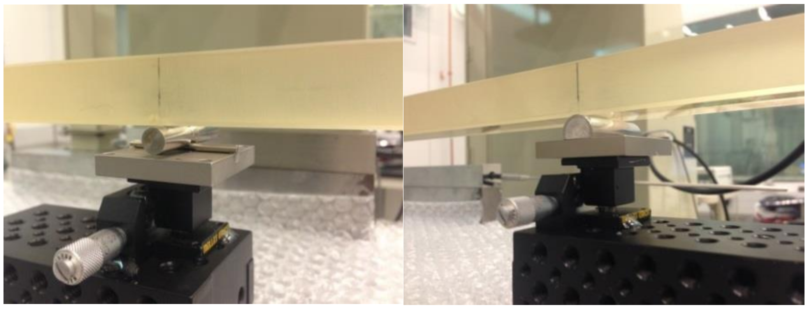


Fig. 5 Scale mounting technique

3.2 Measurement

A scale is placed on adjustable stages and located at the Bessel points where the scale will have minimum bending. One Bessel point support is a fixed half cylinder which constrains the scale in the X-Y plane but allows x-pitch, and the other is a full cylinder allowed to translate along the X-axis but fully constrain the x-pitch. (Fig. 5) Before the program starts, we manually locate the focus of each line, record the X, Y, Z positions, and save the positions. Our main LabView program runs on a Windows 7 desktop machine. The LabView program commands the M48 to move to each of the recorded X, Y, Z positions. At each position, the program commands the camera to take images, and simultaneously commands the laser to repeatedly record the camera position during exposure. After taking the image, the program reads temperature, pressure, and humidity values from the instruments, before the CMM moves to the next line. In order to eliminate the system drift, we measure the scale forward and back, and then average the two passes for a final result.

3.3 Camera Calibration

While the procedure described above will capture images of the line along with the laser readings, evaluating the position of the center of line in linear units still requires the calibration of the camera. We perform this calibration in-situ by obtaining multiple images at very close positions on the table, thus obtaining a number of pixel position and laser reading pairs. We then perform a least-squares fit to determine the actual coordinate of the line-center. For purposes of detail, our camera images and laser readings are acquired at 9 positions around the nominal in the following sequence: 0 µm, +5 µm, +10 µm, +5 µm, 0 µm, -5 µm, -10 µm, -5 µm, 0 µm. (Fig. 6) The center position is measured three times, the two positions at +/-5 µm are taken twice and the two positions at +/-10 µm are taken once. This choice of locations favors the center line measurement in the fit and symmetrically samples small positioning errors due to machine approach direction, and also samples small image distortion due to different field of view. Each point taken is a pseudo-null measurement. The slope of the line is the calibrated x-pixel size and the intercept is the measurement. (Notice that the x-pixel size is irrelevant to the measurement.) This technique eliminates the requirement of the old LSI to position and hold the zero position while recording the laser.

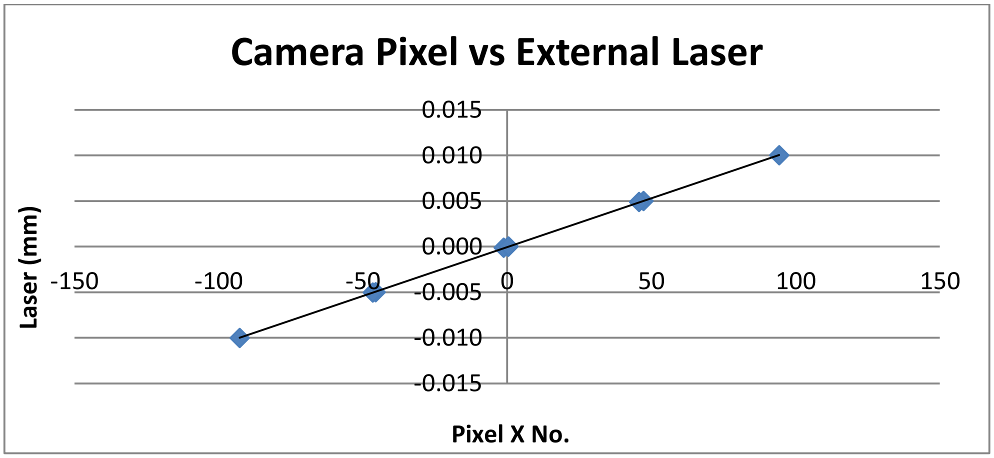


Fig. 6 Camera pixel value vs External laser reading at first line position

3.4 Data analysis

The laser position measurement is based on the refractive index of air for a given wavelength of light and given atmospheric conditions. Our calculations are performed using an updated version of the Edlén equation [6] [7] as a function of air temperature, pressure and humidity input parameters to improve the accuracy of the laser reading. We also record the free-air distance from the interferometer to the retro-reflector at zero fringe count to correct for deadpath changes present in each laser reading. Since the retro-reflector is mounted about 3 mm above and 3 mm behind the focal point, machine X-axis pitch must be known in order to correct for their effects. The known X-axis pitch is measured through in house error mapping technique.

3.5 Repeatability and Performance

We measured two scales using the new NIST LSI system, a 500 mm Mitutoyo Zerodur[1] scale and a 500 mm Bausch&Lomb Glass[1] scale. Each scale is measured multiple times. Both scales have long term in-house measurement history. The deviations from the mean for each run (Table 1&2) show the pool standard deviation less than 10 nm. Comparing to old LSI results measured in 2009 and 2015, both scales agree to within 120 nm on 500 mm line (Fig. 7&8). There is different deviation between 100 mm and 400 mm lines compared to the old LSI data. We suspect the difference between those lines may be related to the fact that the new LSI system focuses on each line we measure, however, the old LSI only focuses on the first and last line.

3.6 Conclusion

This paper describes recent efforts at NIST to develop an alternative to the old LSI system. We describe hardware and measurement control design used in our LSI that helps reduce system uncertainty significantly. Some key attributes are:

a. We correct the refractive index of air real time by monitoring the atmospheric conditions during image acquisition.
b. We accurately align the scale artifact with measurement line thus reducing the contribution of major error sources.
c. By measuring the laser and acquiring camera images at nine steps in and around the nominal position, we significantly improve system reliability.

3.7 Future work

There are some additional hardware and software improvements that can be made in the new NIST LSI system, such as software controlled camera autofocus function and software controlled lighting system. We also plan to develop a detailed uncertainty budget in the near future.

4. Acknowledgements

We would like to acknowledge Bala Muralikrishnan, Eric Stanfield, John Stoup, and Tsai Hong Hong for reviewing the manuscript and suggesting many useful changes and corrections.

5. References

[1] J. S. Beers, Length Scale Measurement Procedures at the National Bureau of Standards, NBSIR 87-3625 (1987).
[2] W. B. Penzes and J. S. Beers, Evolution of Automatic Line Scale Measurement at the National Institute of Standards and Technology, Proc. Of the Symposium on Measurement and Inspection in Industry by Computer Aid Laser Metrology, IMEKO TC Series No. 28, 41-58 (1990).

[3] J. Stoup and T. Doiron, The Accuracy and Versatility of the NIST M48 Coordinate Measuring Machine, Proc. SPIE Vol. 4401 (2001).
[4] NI Vision, NI Vision Concepts Manual, June 2011, 372916L-01.
[5] J. S. Beers and W. B. Penzes, The NIST Length Scale Interferometer, Journal of Research of the National Institute of Standards and Technology, Volume 104, Number 3, May-June 1999.
[6] B. Edlén, Equation for the Refractive Index of Air, Metrologia 2(2), 71-80 (1966).
[7] K. P. Birch and M. J. Downs, An updated Edlén equation for the refractive index of air, Metrologia 30, 155-162 (1993).

Table 1: 500 mm Mitutoyo Zerodur scale deviation from mean

Nominal (mm)	Run 1 (nm)	Run 2 (nm)	Run 3 (nm)	Run 4 (nm)	Run 5 (nm)
0	3	1	-1	-3	1
100	-4	4	-3	1	2
200	2	-3	-2	3	0
300	4	-4	-2	5	-3
400	1	1	-2	2	0
500	5	3	1	-4	5

Table 2: 500 mm Bausch&Lomb Glass scale deviation from mean

Nominal (mm)	Run 1 (nm)	Run 2 (nm)	Run 3 (nm)	Run 4 (nm)	Run 5 (nm)
0	3	-1	-1	3	-5
100	-9	-2	4	5	2
200	-3	-1	1	4	-1
300	0	4	-6	4	-2
400	2	6	-7	9	-10
500	3	-2	-3	10	-8

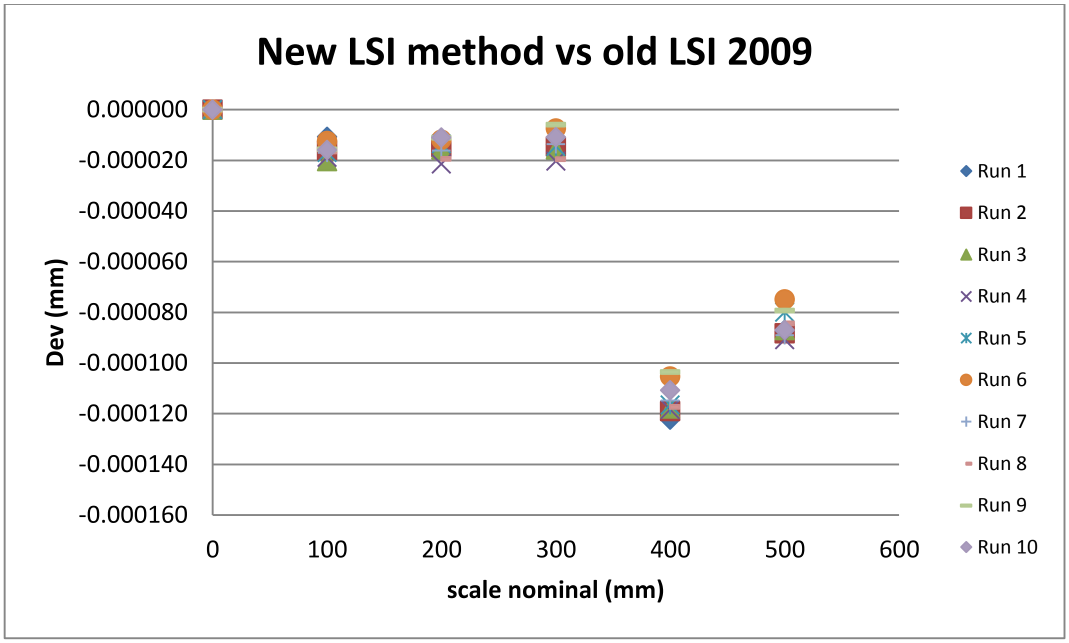


Fig. 7 Mitutoyo 500 mm Zerodur scale measurement result

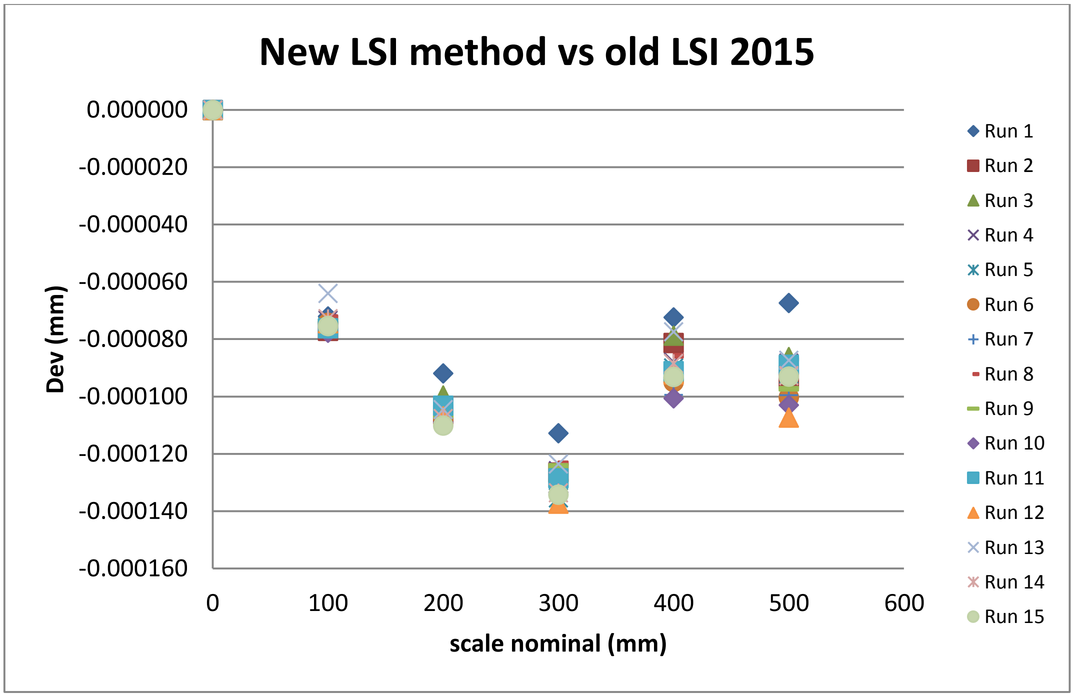


Fig. 8 Bausch&Lomb 500 mm Glass scale measurement result

Catalyzing the Internet of Things and Smart Cities: Global City Teams Challenge

Sokwoo Rhee
Smart Grid and Cyber-Physical Systems Program Office
National Institute of Standards and Technology
Gaithersburg, MD, USA
sokwoo.rhee@nist.gov

***Abstract*— Many smart city and Internet of Things (IoT) solutions are suffering from fragmentation and lack of economies of scale. To address this issue, the National Institute of Standards and Technology (NIST) initiated the Global City Teams Challenge (GCTC) to catalyze collaboration among different stakeholders. The goal is to design and deploy IoT and smart city solutions that are replicable, scalable, and sustainable, thereby leading to the identification and adoption of a consensus framework for smart city technologies. The second round of GCTC is currently in its first phase. Future smart city projects would benefit from a widely distributed IoT communications fabric that can serve as an infrastructure for the deployment of truly sharable and replicable smart city solutions.**

***Index Terms*—Internet of Things, Smart City, Global City Teams Challenge, GCTC, Replicability, IoT Fabric**

I. Introduction

The concept of Cyber-Physical Systems (CPS) or Internet of Things (IoT), which has been around for more than a decade [1], is currently creating a great deal of buzz in the marketplace and media, with a promise to enhance the way we live our lives. There are three major arenas for IoT applications—in the consumer, industrial, and public sectors. Recent interest has mainly focused on the consumer side, including consumer appliances, home area networks and other applications Industrial applications are promising to improve business outcomes for many sectors, including manufacturing, asset management and healthcare.

In the case of public sector applications, the Internet of Things is a major enabling concept to accelerate the development and deployment of smart city solutions. This article discusses the overall architecture of IoT and the issues of current practice of smart city deployments. The article then presents a new collaborative approach that uses the concept of a "challenge" for the acceleration of broader and faster adoption.

II. IoT and Smart Cities Architectures

To understand the basic characteristics of IoT and smart cities, it is useful to analyze the composition of a typical IoT solution and show how the architecture can be mapped to that of smart cities. Figure 1 illustrates a simplified layered architecture of IoT.

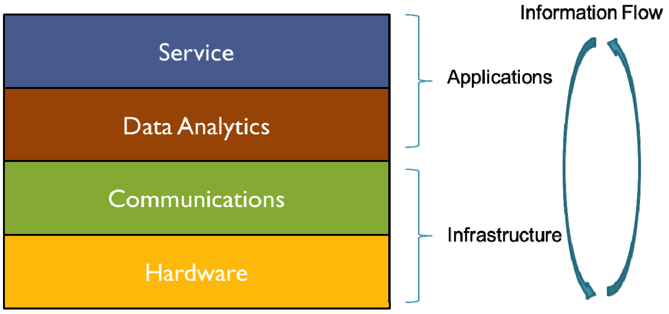


Figure 1: Simplified IoT and Smart Cities Architecture

At the bottom of the structure is the **Hardware layer**, where tangible hardware elements such as sensors, actuators, chips, and radios are found. The elements in this layer typically interact directly with the environment, with other hardware elements, or sometimes with the users/consumers.

The next layer is the **Communications layer**, which is sometimes called "connectivity." This layer connects and binds different components in the Hardware layer so that information can flow between layers or between hardware components. This is where well-known technologies such as Ethernet, Wi-Fi, cellular, and short-range wireless are found. For some applications, the Communications layer is minimal (e.g., scaled down to an internal bus or to simplified connectivity among different hardware components).

The next layer is the **Data Analytics layer**. This layer receives data from the Communications layer, and then stores, analyzes, and processes them. This is where "big data" applications could reside, for example, in the case of applications that require collection and analysis of data from a large number of sources. However, it should also be noted that this layer could be relatively thin and simple, especially in the case of embedded applications. In other words, the Data Analytics layer does not necessarily imply the need for a huge database and an extremely fast processor.

Many distributed IoT-based control systems employ a relatively small-scale Data Analytics layer. An example of a small-scale layer can be found in a smart thermostat that could also function as a local decision maker within the home network.

On the other hand, many IoT solutions deployed at a city-wide scale may require a big centralized data repository and more powerful processors to handle a larger amount of data from multiple sectors and applications. An example of such a system could be a city's disaster command center that is designed to provide simultaneous visibility into different departments (e.g., water, energy, transportation, healthcare, etc.).

The main function of the Data Analytics layer is to collect data from the lower layers and extract useful information from the set of data. Note that the set of data itself may not have significant value and may not be very useful to the user. The information extracted from the data, however, could be valuable in taking actions and achieving a desired end result.

The top layer is the **Service layer**. This layer is where intelligence resides and decisions are made. This layer receives information from the Data Analytics layer, and then makes decisions on next steps. The next steps could include displaying the information on a monitor screen or operating and controlling actuators. The Service layer is important because it is in the position in the architecture to create the highest value for the users of the system. Many business decisions are made in this layer, including human-in-the-loop actions. The human-machine interface can be an important factor in this layer.

Once the decision of the next step is made at the Service layer, sometimes (but not always) information starts flowing in the reverse manner (i.e., from Service layer down to the Hardware layer). This is especially true for systems based on some type of autonomous control. On the other hand, it is sometimes a human being who makes the decision and executes it. In either case, the end result is some type of action that closes the loop of the information flow. A similar representation of IoT data flow was proposed in another article [2].

Many developers consider IoT to be the combination of just the two bottom layers (Hardware and Communications). It is important to note, however, that these two layers are merely a part of the whole IoT architecture. In many cases, the top two layers (Data Analytics and Service) play more important roles in defining and producing the real value from the system. Also in many cases, the design and implementation of the top two layers may be more complex and unclear than the bottom two layers. In many cases, the top two layers are heavily coupled with business cases that are important factors in determining sustainability and replicability of the solutions.

In the case of smart city applications, it is often easier to conceptualize the architecture as two groups of layers—Infrastructure and Applications. "Infrastructure" typically refers to the bottom two layers of the IoT architecture, and "Applications" refers to the top two layers. In some cases, however, the Data Analytics layer could belong to the infrastructure group, depending on the nature of its functionality. Many solutions/products that belong to the application group have more flexibility in deployments than the ones belonging to the infrastructure group. This simple IoT architecture can serve as an initial template to map different smart city solutions to build consensus on their technical interoperability, which is essential in addressing the challenges in accelerating the market momentum for IoT and smart cities..

III. Challenges for Advancing IoT in Cities

Smart cities use smart technologies such as IoT and CPS to improve the quality of life of the residents and citizens. Although progress in deploying IoT solutions has been quite impressive, the IoT market still suffers from the issue of "fragmentation, [3]" and the smart city market shares similar concerns. Many smart city solution projects are isolated and heavily rely on custom-solution developments. Naturally, many of them are "one-off" projects with heavy emphasis on customization and inadequate consideration for future upgradability and extensibility. As a result, these deployments are isolated and do not enjoy economies of scale. Although many cities share the same issues (i.e., parking problems, traffic jams, air pollution, etc.), they often do not share best practices and end up reinventing the wheel. In this landscape, it is very difficult to create common standards for development and deployment of interoperable solutions.

IV. Global City Teams Challenge

To address this issue, the National Institute of Standards and Technology (NIST) has teamed up with US-Ignite and private sector partners to create the Global City Teams Challenge (GCTC) program [4][5]. The goal of GCTC is to establish and demonstrate replicable, scalable, and sustainable models for incubation and deployment of interoperable, standards-based IoT solutions and to demonstrate measurable benefits in smart communities/cities. "Replicability" means that the solutions should be designed to operate in more than one city or community with minimal customization. "Scalability" means that the solution should be functional regardless of the size and volume of the deployment. "Sustainability" means that the project should be designed to last beyond its initial funding stage. In other words, the deployed solution must either (1) create its own revenue to support the operational cost or (2) provide enough tangible benefits that the municipal governments are willing to cover the operation cost using their budgets. Many of today's smart city deployments lack one or more of these characteristics. GCTC places significant emphasis on the ability to measure tangible benefits for residents and citizens, thus empowering leaders within communities to demonstrate the benefits of adoption.

A. Approach

To achieve the goal of GCTC, the program was designed to create a voluntary environment for multi-stakeholder collaboration. As can be seen in Figure 2, multiple cities and technology innovators are brought into the program and asked to coalesce around shared challenges (e.g., air pollution, traffic management, emergency response) to create teams called "Action Clusters." Each Action Cluster creates a project plan with a timeline to demonstrate their accomplishments in a tangible manner. Because each action cluster includes multiple members, it is likely that the outcome of the solution will be replicable to other cities. In the case that a team has only one municipal partner, the team is encouraged to establish additional partnerships with other cities by demonstrating measurable and quantifiable benefits of the solution. It is also important to note that replicability and interoperability should be based on collaboration that is global rather than just regional.

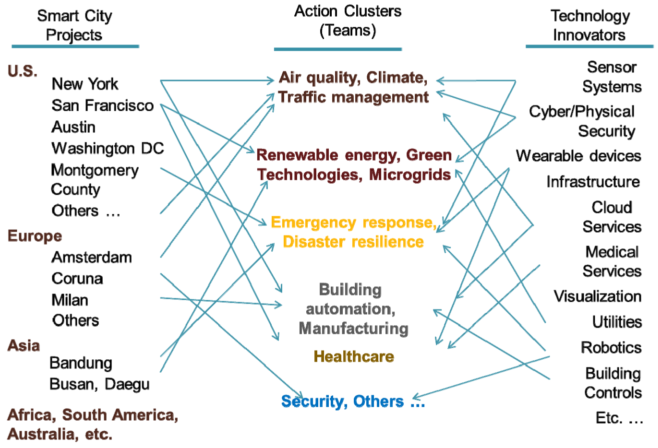


Figure 2: GCTC Approach

Cities have two strong reasons for participating in GCTC. For the cities that have already gone through successful deployments, it is an opportunity to promote their solutions and be the origin of replication for other cities that are facing similar challenges. For the cities that are just starting to consider the deployment of smart city solutions, it is an opportunity to learn from other cities' projects and to showcase their own city as a ready partner to organizations with replicable smart city technologies.

For corporations, GCTC is an opportunity to identify new business partners, demonstrate their proven solutions, and enlarge their market.

Academic institutions participate in order to find opportunities for joint R&D with cities/communities and partners that will enable the joint development and deployment of new technologies. The process also allows researchers to identify key common characteristics and components among different applications and implementations, which will help the market to find convergence on best practices and eventually lead to broadly adopted standards.

B. GCTC 2015

The first round of GCTC culminated on June 1, 2015, after a nine-month-long process of team building, incubation, solution development, and deployment. More than 60 teams, composed of over 200 organizations and three dozen cities/communities around the world, gathered at the National Building Museum in Washington, D.C., to present and demonstrate the impact of their smart city solutions. Many high-profile visitors and speakers, including King Willem-Alexander and Queen Maxima of the Netherlands and U.S. Secretary of Transportation Anthony Foxx, came to celebrate and encourage the teams' accomplishments. The event was attended by over 1300 people and was covered by many media outlets.

C. GCTC 2016-2017

Based on the success of GCTC 2015, the next round was launched in November 2015. This new GCTC round is composed of two phases. The first phase will continue until June 2016, with the focus on building the teams and defining the project goals, timelines, and Key Performance Indicators (KPI) of the quantifiable impacts to residents and citizens. Participants will demonstrate and pilot the solutions and will build partnerships with as many cities as possible. The second phase will focus on deploying the solutions, achieving the goals (based on the KPIs devised during Phase 1), and measuring the impacts. Phase 2 will culminate in June 2017.

GCTC 2016-2017 carries over the key elements of GCTC 2015, and adds two more ambitious goals, encouraging the teams to:

- deploy the shared and replicable solutions in multiple cities, potentially on multiple continents and
- provide tangible measurements of the improvements made by the solutions, such as reduction of average commute time, reduction of air pollution, reduction of water loss.

V. Further Discussions: IoT Smart City Fabric

One of the missing links in accelerating the deployment of IoT/CPS and smart city solutions is the lack of a "connectivity fabric"--a commonly shared IoT/CPS network infrastructure among cities and communities [6]. As of today, there is no easy mechanism for an IoT solution to be deployed and become operational in a plug-and-play manner. For example, a simple flood-level sensor deployed in one city may not share the same backbone infrastructure required to exchange data with sensors in other cities. The current landscape of IoT and smart city is similar to that of the communications infrastructure of pre-Internet days.

It is essential that a communications fabric infrastructure be developed that can enable IoT devices and smart city solutions to identify and communicate in a plug-and-play manner, to create synergy between sectors, to reduce overhead, and to catalyze the mass adoption of affordable solutions by the residents in cities and communities. The IoT/Smart City fabric would enable sharing and replication of the solutions beyond the city limit, just as the Internet broke the physical-distance barrier for communications and commerce. Combined with multi-stakeholder collaboration programs such as GCTC, the IoT/Smart City fabric—built to be open and neutral--could allow many cities and communities, large and small, to enjoy the benefits of advanced technologies to improve the quality of life.

Starting with its Challenge programs [7][8], NIST has already taken steps in the direction of promoting consensus around reference architectures for interoperability. Informed by GCTC, NIST has taken the first step to establish an international technical public working group to help develop an "IoT-Enabled Smart City Framework." [9]

Acknowledgment

We would like to acknowledge the National Science Foundation, U.S. Department of Transportation, International Trade Administration, and all other partners and participants for their support and contribution to GCTC.

References

[1] Industry Advisory Board, RWTH Aachen University, "Cyber-Physical Systems - History, Presence and Future," February 2013.
http://www.ima-zlw-ifu.rwth-aachen.de/fileadmin/user_upload/INSTITUTSCLUSTER/Publikation_Medien/Vortraege/download//CPS_27Feb2013.pdf

[2] E. P. Goodman, Rapporteur, "The Atomic Age of Data: Policies for the Internet of Things," Communications and Society Program, The Aspen Institute, 2015, p. 5.
http://csreports.aspeninstitute.org/documents/Atomic_Age_of_Data.pdf

[3] M. Smolaks, "Internet Of Things In Danger Of Fragmentation" TechWeek Europe, July 2013
http://www.techweekeurope.co.uk/workspace/internet-of-things-in-danger-of-fragmentation-120566

[4] Global City Teams Challenge
http://www.nist.gov/cps/sagc.cfm

[5] Global City Teams Challenge
https://www.us-ignite.org/globalcityteams/

[6] S. Rhee, G. Mulligan, "SmartAmerica Challenge," 2013-2014, p. 6.
http://www.nist.gov/el/upload/Smart-America-Challenge-r1-25p.pdf

[7] E. P. Goodman, Rapporteur, "The Atomic Age of Data: Policies for the Internet of Things," Communications and Society Program, The Aspen Institute, 2015, p. 48.
http://csreports.aspeninstitute.org/documents/Atomic_Age_of_Data.pdf

[8] S. Rhee, "Internet of Things and Global City Teams Challenge," January 2015, p. 33.
http://www.nema.org/Policy/Documents/IoT%20Global%20City%20Summary_NEMA_Sokwoo%20Rhee_01.08.2015.pdf

[9] International Technical Working Group on IoT-Enabled Smart City Framework
https://pages.nist.gov/smartcitiesarchitecture/

A Long Term Evolution (LTE) Device-to-Device module for ns-3

Richard Rouil, Fernando J. Cintrón, Aziza Ben Mosbah, and Samantha Gamboa Quintiliani

National Institute of Standards and Technology
Gaithersburg, MD
{richard.rouil, fernando.cintron, aziza.benmosbah, samantha.gamboaquintiliani}@nist.gov

ABSTRACT

In this paper, we provide an overview of our on-going implementation of a 3rd Generation Partnership Program (3GPP) Proximity Services (ProSe) module in ns-3 to enable the performance evaluation of device-to-device (D2D) discovery and communication in Long Term Evolution (LTE) networks.

CCS Concepts

• Networks → Network performance evaluation • Networks → Network types → Mobile networks.

Keywords

3GPP; Long Term Evolution; Device-to-Device communication; network modeling; ns-3.

1. INTRODUCTION

Device-to-device (D2D) communication is a common feature in technologies such as Bluetooth and WiFi. However, this is a fairly new concept for 3GPP where historically access to the radio resources has been controlled by the network. If the network is not available, the devices are not able to communicate. With Release 12 and the introduction of ProSe [1], 3GPP provides the ability for User Equipments (UEs) to discover each other and, in some cases, communicate with each other without eNodeB intervention. The discovery service provided by ProSe responds to the increasing use of social media where users want to know what is happening around them. Some of the use cases include advertisement broadcast in shopping malls or notifications of nearby people with similar interests. While discovery is available to all UEs when the network supports it, direct communication is currently restricted to Public Safety users, which have identified this feature as critical in order to fully transition to LTE. Furthermore, D2D communication has been identified as one of the enablers for 5G communications [2] indicating that further research is needed in that domain and that the current restrictions may have to be removed. The rest of this document provides an overview of the ProSe module implementation followed by validation results, open issues and future work.

2. IMPLEMENTATION

Our ProSe module is extending the ns-3 LTE model [3] by adding UE to UE communication capabilities. In 3GPP specifications, the term sidelink refers to the D2D communication in contrast to downlink and uplink communication between the eNodeB and the UE.

Pursuant to Title 17 United States Code § 105, works of the United States Government are not subject to copyright protection within the United States. Pursuant to this Agreement, Publisher is hereby granted the unlimited right to print, publish, prepare derivative works and distribute the Work, or the National Institute of Standards and Technology (NIST) contribution to the Work, in any medium, or authorize others to do so on your behalf, on an unrestricted royalty-free basis throughout the World. To the extent the United States Government may claim foreign copyright, no assignment of rights is made.

2.1 Architecture

In our implementation, the structure of the LTE UE nodes, shown in Figure 1, has not been changed. However, the extension involved some modifications at all levels of the LTE protocol stack, from the Non Access Stratum (NAS) down to the physical layer. The main design alteration, shown in Figure 2, was the addition of a new instance of the *SpectrumPhy* class in the UE in order to allow the reception of packets sent by other UEs on the uplink channel.

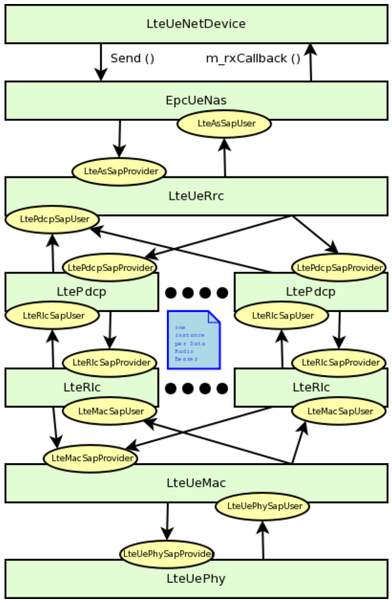


Figure 1: LTE radio protocol stack architecture for the UE on the data plane

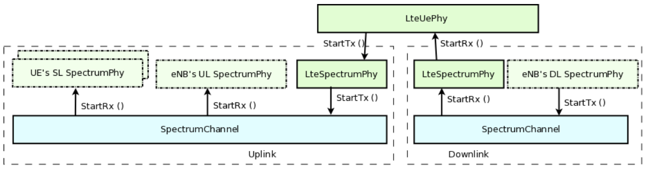


Figure 2: New PHY and channel model architecture for the UE

Rouil, Richard; Cintron, Fernando; Ben Mosbah, Aziza; Gamboa Quintiliani, Samantha.
"An LTE Device-to-Device module for ns-3."
Paper presented at the WNS3, Seattle, WA, Jun 15-Jun 16, 2016.

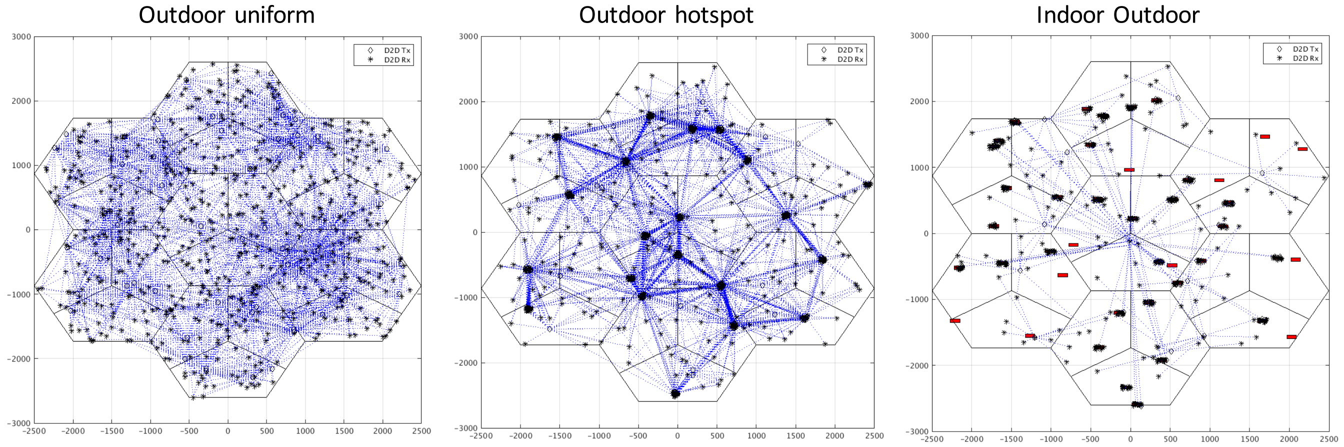


Figure 3: Topologies used for model validation

2.2 Summary of modifications

2.2.1 Radio Resource Control (RRC) Protocol

The RRC layer provides signaling between the eNodeB and the UE to perform attachment and setup radio bearers. Extensions to the protocol have been made so the UE can indicate its interest in performing D2D when in coverage of an eNodeB. It also stores the preconfigured radio resources when the UEs are out of coverage.

2.2.2 Packet Data Convergence Protocol (PDCP) and Radio Link Control (RLC) Protocol

The sidelink radio bearers use the Unacknowledged Mode (UM) transmission mode that is already available in ns-3. However, the identifier for the logical channels has been extended to include the source L2 ID and destination L2 ID that identifies the transmitter UE and the group to which the packets must be delivered.

2.2.3 Medium Access Control (MAC) Protocol

The MAC protocol responsible for allocating radio resources had to be modified at both the eNodeB and the UE. The changes include the processing of sidelink Buffer Status Request (BSR) to indicate how much D2D traffic needs to be transmitted and the schedulers to handle the new type of resource allocations. The concept of scheduling algorithm is new to the UE implementation as it normally just follows the information provided by the eNodeB at each subframe. With D2D, the UE has to decide how to allocate resources when it is out of coverage or when it is in coverage but the allocation mode is UE selected. The initial scheduler implementation provides a static allocation, with the same number of resource blocks and subframes used in each sidelink period, that is configurable from the scenario.

2.2.4 Physical Layer Protocol

The physical layer was extended to support additional physical channels such as the Physical Sidelink Discovery Channel (PSDCH) to send and receive discovery messages, Physical Sidelink Control Channel (PSCCH) to carry the allocation information, and Physical Sidelink Shared Channel (PSSCH) to carry the D2D data. The model also supports scanning and transmission of sidelink synchronization messages so UEs can detect and synchronize with each other. Finally, a half-duplex constraint has also been added so UEs cannot send and receive uplink/sidelink transmissions as the same time.

2.2.5 Propagation and Error Modeling

Several D2D propagation models have been implemented as specified by 3GPP [4] to model outdoor to outdoor, outdoor to indoor, and indoor to indoor environments. A new error model was introduced to handle interference from multiple sources on the same resource blocks and to properly characterize uplink modulations.

3. VALIDATION

A critical step for the adoption of a new model is to compare the results obtained using well defined scenarios. This section describes the performance evaluation of the sidelink shared (data) channel and shows that our results are within range of other models documented in [4].

3.1 Modeling assumptions

The assumptions contained in Table 1 were used to perform the evaluation of the sidelink shared channel.

Table 1: Simulation parameters

Parameter	Value
Transmission BW (RBs)	2.0
Packet size including CRC (bits)	328.0
Modulation and Coding Scheme	QPSK
Coding	Turbo
Number of symbols/Transmissions	12.0
Tx Power (dBm)	23.0
Num HARQ transmissions	4.0
Frequency Diversity (across transmissions)	Yes [per period]
Time Diversity (across transmissions)	Yes [per period]
Number of TX/cell	3.0
RSRP threshold (dBm)	-112.0
Traffic	On/off Voice over IP (VoIP)

3.2 Topologies

The validation scenarios are based on a 19 macro-cell topology. The UEs are deployed following one of three options: in outdoor uniform, all UEs are uniformly and randomly deployed within each sector; in outdoor hotspot, some of the UEs are concentrated in random locations; finally, for indoor outdoor, buildings are randomly placed in the topology and UEs are deployed either indoor or outdoor. Random transmitters are selected throughout the topology and receiver UEs are associated to the transmitters if the RSRP is above the preconfigured threshold. For legibility, Figure 3 illustrates those deployments for a 7 macro-cell deployment.

3.3 Simulation results

In this section we present the performance results obtained with our model side by side with the results provided in [4]. The first performance metric used is the fraction of successful VoIP links, which is defined by a link with less than 2 % packet loss. As shown in Figure 4, our results are comparable to the other companies.

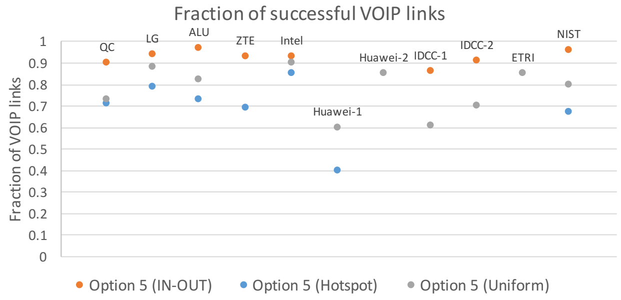


Figure 4: Fraction of successful VOIP links for various deployments

The second metric is the number of successful links per transmitter. As with the fraction of successful links, Figure 5 shows that our results are in the same range as the other companies.

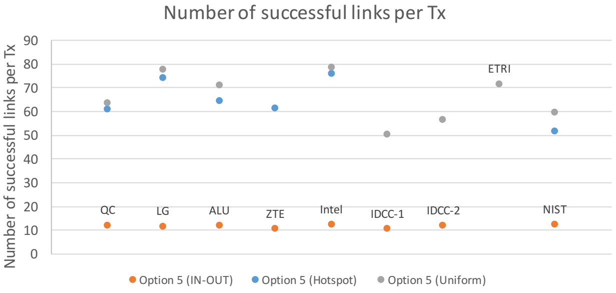


Figure 5: Number of successful links per transmitter for various deployments

4. OPEN ISSUES

Among the model limitations, we can mention the lack of idle mode in the default LTE implementation. Workarounds had to be made to simulate the out of network scenarios. In addition, we would like to create an UE scheduler interface as currently done in the eNodeB so that researchers can easily test their own algorithms. Finally, traces will need to be extended to support the D2D packet transmissions.

5. CONCLUSION AND FUTURE WORK

In this extended abstract, we presented an overview of the extensions made to the ns-3 LTE implementation to support D2D discovery and communication. The model presented is under active development and several new features may be added such as UE-to-network relay or priority queues, which are features added in 3GPP Release 13.

6. REFERENCES

[1] 3GPP TS 23.303 "*Proximity-based services (ProSe); Stage 2"* Nov. 2015. http://www.3gpp.org/DynaReport/23303.htm

[2] B. Bertenyi, "*3GPP system standards heading into the 5G era*" [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1614-sa_5g

[3] N. Baldo, "*The ns-3 LTE module by the LENA project*". [Online]. Available: https://www.nsnam.org/ tutorials/consortium13/lte-tutorial.pdf

[4] 3GPP TS 36.843 "*Study on LTE device to device proximity services; Radio aspects"* March. 2014. http://www.3gpp.org/DynaReport/36.843.htm

Proceedings of the ASME 2016 International Manufacturing Science and Engineering Conference
MSEC2016
June 27-July 1, 2016, Blacksburg, Virginia, USA

MSEC2016-8702

PROMOTING MODEL-BASED DEFINITION TO ESTABLISH A COMPLETE PRODUCT DEFINITION

Shawn P. Ruemler
Purdue University
West Lafayette, Indiana, USA

Kyle E. Zimmerman
Purdue University
West Lafayette, Indiana, USA

Nathan W. Hartman
Purdue University
West Lafayette, Indiana, USA

Thomas Hedberg, Jr.
National Institute of Standards and Technology
Gaithersburg, Maryland, USA

Allison Barnard Feeney
National Institute of Standards and Technology
Gaithersburg, Maryland, USA

ABSTRACT

The manufacturing industry is evolving and starting to use 3D models as the central knowledge artifact for product data and product definition, or what is known as Model-based Definition (MBD). The Model-based Enterprise (MBE) uses MBD as a way to transition away from using traditional paper-based drawings and documentation. As MBD grows in popularity, it is imperative to understand what information is needed in the transition from drawings to models so that models represent all the relevant information needed for processes to continue efficiently. Finding this information can help define what data is common amongst different models in different stages of the lifecycle, which could help establish a Common Information Model. The Common Information Model is a source that contains common information from domain specific elements amongst different aspects of the lifecycle. To help establish this Common Information Model, information about how models are used in industry within different workflows needs to be understood. To retrieve this information, a survey mechanism was administered to industry professionals from various sectors. Based on the results of the survey a Common Information Model could not be established. However, the results gave great insight that will help in further investigation of the Common Information Model.

INTRODUCTION

Model-based definition (MBD) is a strategy for moving from two-dimensional (2D) paper-based drawings to three-dimensional (3D) computer-aided design (CAD) models where the model will contain all the information so that one day drawings may no longer be needed. However, in today's modeling environment, drawings are still used [1]. With advances such as better time-to-market, efficiency, and improved product quality, MBD has gained substantial popularity within the aerospace and defense industry [2]. However, a good majority of companies are not yet convinced on the idea of moving to an environment with no drawings [1].

While MBD has been gaining popularity, several questions remain regarding the full definition of MBD. Standards such as ASME Y14.41 [3] and ISO 16792 [4] exist to document how a model should be defined with annotations. These standards also help in understanding how to interpret the data within the model. However, the standards do not document the required amount of information that the model must contain [5]. It is important to understand what information needs to be communicated when considering moving from drawings to 3D-CAD models so the engineers can continue to do their jobs efficiently.

In today's industry, it is common that several disciplines and enterprises collaborate and share resources to complete various tasks. Elements that describe this type of scenario include entities and connections between the entities. The entities include applications, persons, and enterprises, whereas the connections between these entities include data exchange and collaborations. Product models are crucial in achieving this interoperability within the network of entities [6]. It is important to organize the information that is relevant to the user inspecting or working with the model so that they do not have to sift through layers of unnecessary data [7,8]. Designers from different disciplines usually work on the same models, which can distract them when they interact with design details that are unnecessary to them. Finding a common ground between

This work is in part a work of the U.S. Government. ASME disclaims all interest in the U.S. Government's contributions.

different design disciplines can provide several benefits including protecting sensitive information, enabling collaborative supply chains, and facilitating multi-disciplinary design [9].

This paper is focused on finding the information that is common among different aspects of the product's lifecycle. Design, manufacturing, and quality is the main focus of this paper. Maintenance, sustainment, and decommission will be addressed in future work. Ultimately, all phases of the product's lifecycle will be reviewed – leading to a Common Information Model. Establishing an understanding for what all information needs to be in a 3D-CAD model so it represents and communicates the same level of information as a 2D drawing is key in formalizing the Common Information Model and the main reason why this paper focuses on the early phases of the product's lifecycle.

LITERATURE REVIEW

A review of relevant academic literature has been composed to further investigate MBD and the information that needs to go into a 3D model to relay all the necessary information a drawing traditionally carries as well as how ontologies can be integrated to help product data. A review of frameworks and workflows has also been conducted.

Model-based Definition

MBD is the strategy of moving away from drawings and other means of product definition and moving to 3D-CAD models. This would establish the 3D-CAD model the only source for defining the product and its geometry. Adamski [10, p. 40] talks about the evolution of how MBD came to be:

> "In the past, 2D-drawing sheets with geometric dimensions and tolerances were used to define a part. Next, 3D models with 2D drawings, projection, geometrical dimensions, tolerances were used … So, model based definition includes one system file, model 3D geometry, GD&T [geometric dimensioning and tolerancing] data with notes and comments such as base coordinate system, dimensions, tolerances, flag notes and technical comments concerning material, surface smoothness, weight and general notes. Model-based definition is a process that allows the design team to input all their information into the 3D model, thus eliminating the need to create a drawing."

Traditional drawings have been used in industry to communicate design because they are easy to understand. The engineering drawing's main purpose is to carry and maintain product definition in a way that no assumptions or misinterpretations can be made. However, CAD software's development over the past decades has helped with the production of engineering drawings. Product development within CAD systems has become the standard and engineering drawings are no longer used as the primary product-definition source [1].

MBD is not widely utilized yet within industry [10,11]; however, it is gaining popularity in engineering and manufacturing environments due to a wealth of benefits [2]. The benefits of MBD include reduction in manually reproduced data, reduced errors in design, better communication, quicker response times, fewer files to maintain, and reductions in cost [10,11].

Domain Ontologies

Anderson and Vasilakis [12, p. 11] define an ontology as "a rigorous conceptual model of a specific domain." These conceptual models have several contexts including "advanced information retrieval, knowledge sharing, web agents, natural language processing, and simulation and modeling." Ontologies can either be domain specific or general. Domain specific ontologies model information used in a specific setting, while a general ontology serves several domain-specific ontologies [12].

Anderson and Vasilakis [12, p. 14] take their definition of an ontology further by stating:

> "An ontology embodies some sort of world view with respect to the given domain. The world view is often conceived as a set of terms (e.g. entities, attributes, and processes), their definitions and inter-relationships; terms denote important concepts (classes of objects) in the domain. This is referred to as conceptualization. Recording such a conceptualization with an ontology is referred to as ontology development."

The benefits to ontologies are they share a common understanding of information in knowledge domains, and they can improve interoperability within applications that use domain knowledge. Ontologies make assumptions explicit so applying changes is easier as assumptions evolve, and they enable re-use of domain knowledge, which means the ontology can be used by multiple applications [12]. Ontologies help bridge the gap of data interoperability between different software systems and assist the communication between software systems during a product's lifecycle. Ontologies can be used with standard file formats to allow various data types to be contained with a product, which can help convey design intent. Using ontologies with standard file formats is also good for long term archival [13].

Frameworks

A framework is created to help support a product throughout all phases of the product's lifecycle. The framework is to help information flow and be obtained through the different phases of the lifecycle. Frameworks for PLM have been deployed to help integrate business and technical information systems. They also allow partners to collaborate effectively when creating products. According to Srinivasan [14, p. 464] these frameworks:

> "Allow engineering and business objects and processes to be built or composed as modular pieces of software in the form of services that can communicate with each

> other and be used across different parts of a business. These modular software pieces can be reused and reconfigured in new ways as business conditions change, thereby saving time and money for companies."

When used in a PLM system, a framework is "intended to capture product, design rationale, assembly, and tolerance information from the earliest conceptual design stage…to the full lifecycle" [15, p. 1399]. According to Sudarsan et al. [15, p. 1402], the National Institute of Standards and Technology (NIST) information modeling framework has the following attributes:

> "It is based on formal semantics, and will be supported by an appropriate ontology to permit automated reasoning; it is generic; it deals with conceptual entities such as artifacts and features, and not specific artifacts such as motors, pumps or gears; it is to serve as a repository of rich variety of information about products, including aspects of product description that are not currently incorporated; it is intended to foster the development of novel applications and processes that were not feasible in less information-rich environments; it incorporates the explicit representation of design rationale, considered to be as important as the product description itself; and there are provisions for converting and/or interfacing the generic representation schemes with a production-level interoperability framework."

The NIST information modeling framework's implementation will provide a repository of all product data and information from every stage of the design process. The framework will serve all product description data to the PLM system using a single information exchange protocol, and "support direct interoperability among CAD, CAE, CAM and other interrelated systems where high bandwidth, seamless information interchange is needed," [15, p. 1399].

The NIST information modeling framework contains four components. These components are the Core Product Model (CPM), the Open Assembly Model (OAM), the Design-analysis Integration Model (DAIM), and the Product Family Evolution Model (PFEM). The CPM establishes a base-level, generic product model. It is capable of capturing the entire context commonly shared in development. According to Sudarsan et al. [15, p. 1404-1407], the OAM establishes "a standard representation for exchange protocol for assembly and system-level tolerance information." The DAIM is "a conceptual data architecture that provides the technical basis for tighter design-analysis integration than is possible with today's tools and information models." Lastly, the PFEM "represents the evolution of product families and the rationale of the changes involved."

Workflows

Understanding how information flows throughout a company and through different processes is crucial knowledge. Workflows are an important technology. There are a vast amount of tools that support workflow design. Having a good workflow can help share data efficiently. Good workflows can also help workers find where data was created and understand how the "original source of data was used [16, p. 537]."

A primitive science of workflow designs contains workflow orchestration, workflows, and workflow instances. According to Deelman et al. [16, p. 528], "workflow orchestration refers to the activity of defining the sequence of tasks needed to manage a business or computational science or engineering process." A workflow is a template for the workflow orchestration and a workflow instance refers to the specific workflow of a problem, which includes the definition of input data. In a science and engineering environment, these terms have a broader meaning and can be spread out into four areas. These four broad areas are composition, mapping, execution, and provenance. Composition, representation, and data model refer to the composition of the workflow using means such as text, graphics, etc. Mapping is defined as "mapping from the workflow to underlying resources [16, p. 529]." Execution is the "enactment of the mapped workflow on the underlying resources [16, p. 529]." Metadata and provenance refers to "the recording of metadata and provenance information during the various stages of the workflow lifecycle [16, p. 529]."

Common Information Model

A Common Information Model represents details that are relevant in different versions of models including design, manufacturing, and quality models. Within these models used in different workflows are domain specific elements. The Common Information Model will contain the information that is common amongst these different domain specific elements. To reach a Common Information Model, several sets of information will need to be understood. In an MBD environment, the model is the main knowledge artifact for product definition – what information a MBD needs to provide must be known. Also, in certain circumstances, different disciplines in industry will use the same model, but require different perspectives or contexts of the model. Breaking the data up across different platforms can be a challenge, but beneficial to the users. Bouikni et al. [7, p. 71] state "generating an appropriate view makes it possible to provide a favorable environment to the actors, where information is targeted in quantity and in contents to be adapted to the requirements of the task." To understand what information is common among different versions of models such as design, manufacturing, and quality, the information that goes into an MBD environment must be understood.

What Needs to Go In. Before attempting to establish a Common Information Model, it is important to understand what information needs to be in the 3D-CAD model to be able to communicate the same amount of information as a 2D drawing. Quintana et al. [1, p. 506] point out "significant time and effort is required to properly assess the drawings' replacement," meaning it will not be easy to determine what information needs to be contained within the 3D-CAD model.

GD&T Information. For models to convey all the information contained in drawings, they will need to contain a wide variety of data. MBD should consist of one central knowledge artifact containing 3D geometry with GD&T and functional tolerances and annotations (FT&A). GD&T and FT&A refer to the products dimensions, tolerances, and any other annotations that the model must contain to be correctly interpreted [10].

Relevant Information. Product Lifecycle Management (PLM) is imperative and its core aspects should be consistent for the designer to keep that designer focused on the information that is relevant for a particular phase. According to Bronsvoort and Noort [8, p. 929]:

> "A major goal of integral product development, which is an important aspect of product lifecycle management, is to allow the designer of any development phase to focus on the information that is relevant for that phase, without being diverted by information that is relevant for other phases only. On the other hand, the information for all phases should be integrated, so that no inconsistency can arise."

Basic Characteristics. Companies within industry have certain standards while working with CAD/CAM systems. These standards include layers arrangement, new projects naming and numbering rules, rules for creating drawings, rules for creating 3D-CAD models, rules of creating models of parts machined on computer numerical control (CNC) machines, notes, comments, tolerances, etc. MBD files must contain basic characteristics of the product. These characteristics that must be contained within the model are notes, base-coordinate systems, dimensions, tolerances, flag notes, technical comments regarding material, surface smoothness, weight and other general notes [10].

Information Assurance. Information assurance is critical within each step of a models process through PLM, and there are several information assurance issues in the context of collaborative design. Information assurance creates new problems that need to be addressed accordingly so there can be development of collaborative CAD systems. These issues include protecting sensitive information; enabling collaborative supply chains; facilitating multi-disciplinary design, role-based viewing, and security framework for collaborative CAD and role-based-view generation [9].

Security. Each process of PLM security is extremely important for any company. Certain technologies exist managing digital rights. Organizations such as NIST's Information Technology Laboratory and the World Intellectual Property Organization (WIPO) are creating standards within this area [9].

Standardization. Standardizing product meta-data is crucial for company collaboration and efficiency in production. Product meta-data includes information such as part number, bill-of-material, product-assembly structure, author, approver, supplies, version, and change history. Having this information standardized throughout engineering systems reaches out to other information systems. These systems include Enterprise Resource Planning (ERP), Manufacturing Execution Systems (MES), Customer Relationship Management (CRM), and Enterprise Asset Management (EAM), which leads to an increasing demand for standardization. Srinivasan [14, p. 465] clarifies on this increase:

> "One of the most striking developments in the past few years is the wide-spread acceptance of product meta-data as business objects and the enterprise-wide engineering processes as business processes. This metamorphism, as it were, is profound because it has propelled PLM as an information system of concern from essentially engineering organizations to a much wider business enterprise. This, in turn, has provided the impetus to standardize business objects, and languages for business process modeling and execution."

Singular Data File. A critical part within each process of a Common Information Model is keeping it a singular data file for downstream consumers, in which case can be easily distributed within other areas of other departments such as design, manufacturing and inspection. Briggs et al. [14, p. 11] state:

> "All the data required to define the product are currently captured and available to downstream consumers, such as manufacturing, although these data are actually captured and distributed in a single electronic source. One widely understood benefit of MBD is a significant reduction in manually reproduced data."

Transformation of Information. Aside from what information needs to go into the Common Information Model, another issue that must be addressed is if the model needs to be used in a different software package or if the model will ever need to be translated using a neutral file format. If this is the case, it is important to know what information needs to come out of the model after being translated as opposed to what information actually does come out in the resulting file. It is also important to know and understand what information gets lost in this translation.

METHODOLOGY

To help investigate the Common Information Model, a survey was conducted with industry professionals. This survey was sent out to a large number of industry professionals from multiple companies and locations around the world. This diverse group of industry members helped give a good look into how models are used throughout different industries. The survey helped understand how models are used in different industries and where industry members are when it comes to using models in the place of drawings.

The survey was comprised of a demographics section, which gave background information on from where the results are coming. Questions about how information is received, as well as in what format were asked, and also where models are used in processes. If the respondents to the survey did not use models, the survey ended. If the respondents did use models in their processes, more questions were asked to get a better understanding of how and where. An understanding of where the respondents' level of capability was with using 3D-CAD models in their processes is crucial information for this study. After this, we asked what types of inspections the respondents do in-house, as well as what tools they use. Along with this, respondents were asked what types of manufacturing processes they use. The respondents were asked to give impacts of different issues typically faced within a manufacturing environment. The last set of questions for respondents was on why they have not moved to an MBD environment and the risks involved.

The survey information was collected and observed using charts and graphs. The following section is a summary of the survey results. Conclusions about the survey have been made, as well as recommendations, and will be given after the survey summary.

SURVEY RESULTS

To get an understanding of how models are used within companies, the Promoting Model-based Definition survey was given to industry professionals and returned 37 responses. To give an understanding of the sample being used, some questions were asked regarding the size of their company and where they were located. The largest amount of respondents (38%) worked at a company with more than 500 employees. Most of the responders (86%) are located within the United States, with the majority (75%) being located in the Midwest. The primary role of the respondents within their companies varied greatly as seen in Figure 1. These answers were fairly diverse and ranged from sales, engineering/design, manufacturing/production, quality/inspection, management, as well as others, with the majority coming from engineering/design and management. The respondents who answered "other" possessed roles such as CEO, system analyst, owner, training, and consulting. This range of roles can help provide a diverse look into the questions within the survey.

The respondents were asked how they receive customer order information and were given the following options: drawings only, primarily drawings (with supplemental models), primary 3D-CAD models (with supplemental drawings), and 3D-CAD models only. There were 27 responses for this, and Figure 2 is a breakdown of the responses. Primary drawings with supplemental models was the highest at 44 percent. 3D-CAD models only received just over a quarter of the responses at 26 percent. And drawings only and primary 3D-CAD models with supplemental drawings received 15 percent of the responses each. This shows that drawings are still play a crucial role in the transfer of data with 74 percent of the responses using a drawing somehow. While 85 percent of the responses use 3D-CAD models in some fashion for carrying data, only 41 percent of the responses use the 3D-CAD model as the only or primary source of information.

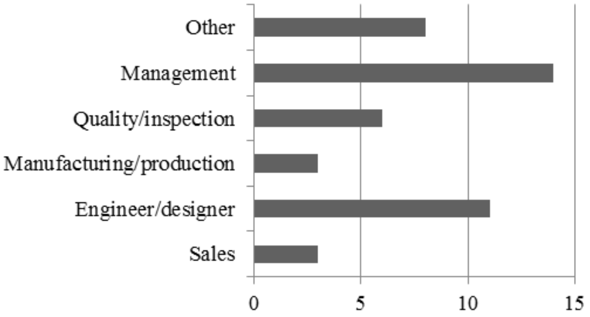


FIGURE 1 - PRIMARY ROLES OF THE RESPONDENTS WITHIN THEIR COMPANY

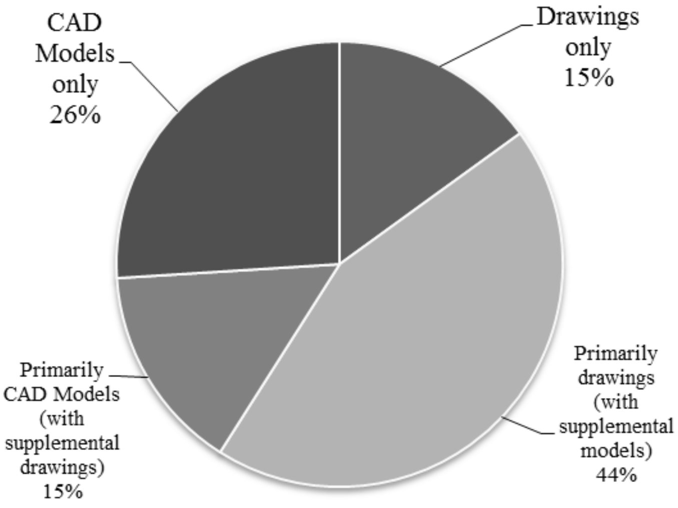


FIGURE 2 - BREAKDOWN OF HOW THE RESPONDENTS RECEIVE CUSTOMER INFORMATION

The next question asked to the respondents was whether or not they would be able to produce a part according to specification if given only a 3D-CAD model and no drawing, which received 25 responses. Figure 3 gives a breakdown of the responses, with only 4 percent of the respondents giving a definite "no". A solid 36 percent responded they could produce the part with no other conditions. The other 60 percent responded they could produce the part to specification; however they would need to interrogate the model manually for dimensional information, with 40 percent of the overall respondents needing to consult with the customer to gather manufacturing and inspection detail.

The respondents had a diverse use for models in their processes. The respondents were to select all the processes for which they use models. There were 26 responses, and most of the options presented to the respondents were selected with high quantities, almost evenly, with CMM/Inspection programs receiving the most selections. Only one respondent selected that they do not use models in their production inspection or processes. Figure 4 gives the distribution of the answers. The two votes for “other” were finite element analysis and design.

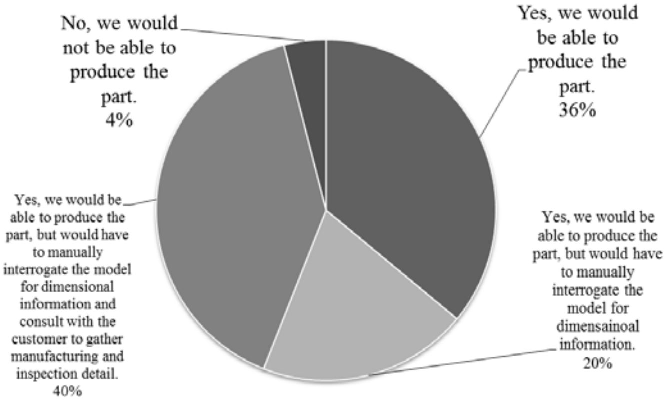


FIGURE 3 - BREAKDOWN OF WHETHER RESPONDENTS WOULD BE ABLE TO PRODUCE A PART TO SPEC GIVEN ONLY A CAD MODEL AND NO DRAWING

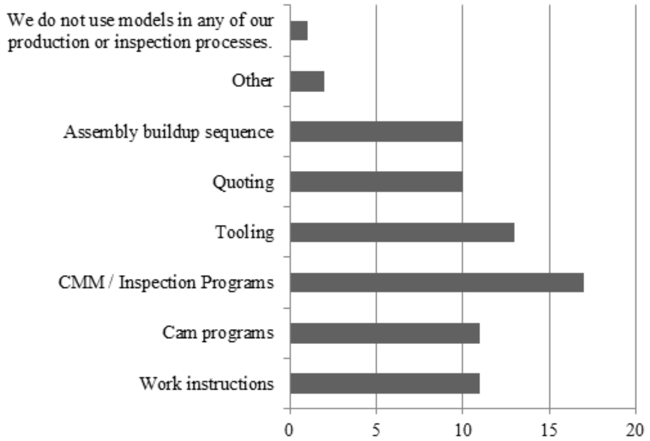


FIGURE 4 - WHERE THE MODELS ARE USED IN PROCESSES

After seeing where the respondents were using models, the respondents were asked in what formats they receive information for making parts and to select all formats that apply. There were 18 responses. Figure 5 shows the responses, with native 3D-CAD model (14) and STEP (11) receiving the most responses.

Knowing how the respondents received information, they were asked what format of information to make parts best suits for their process/needs. Figure 6 gives the distribution of these answers, which came from 18 of the respondents. The options given were native 3D-CAD model, 3D PDF (Portable Document Format), JT (Jupiter Tessellation), STEP (Standard for the Exchange of Product model data), IGES (Initial Graphics Exchange Specification), 2D PDF, DXF (Data Exchange Format), and other. Native 3D-CAD model received the highest selection at 56 percent. The next highest was STEP with 22 percent. 3D PDF, IGES, 2D PDF, and DXF all received 6 percent and there were no selections for JT.

The next question in the survey was regarding what types of inspections were done in house. Again, there were 18 responses. The options were first article inspection (FAI), receiving, in-process, and final. All options received several selections, with FAI, in-process, and receiving getting the most, as seen in Figure 7.

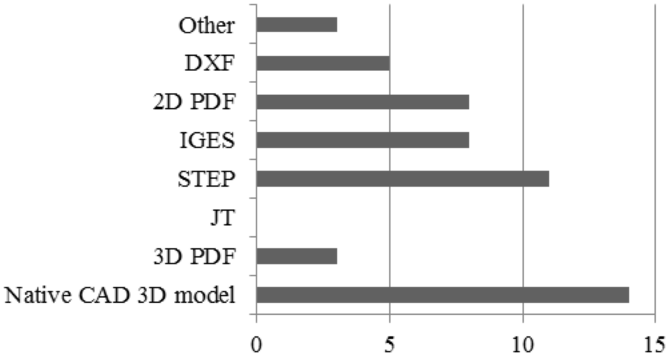


FIGURE 5 - WHAT FORMAT INFORMATION IS RECEIVED IN

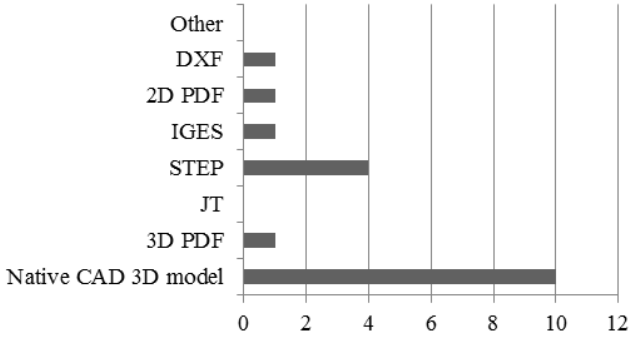


FIGURE 6 - FORMATS OF INFORMATION TO MAKE PARTS BEST SUIT THE PROCESS/NEEDS

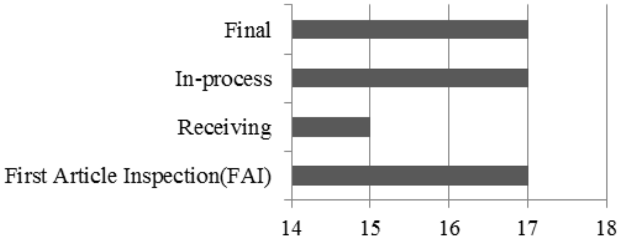


FIGURE 7 - WHAT TYPES OF INSPECTIONS ARE DONE IN-HOUSE

Knowing what types of inspections the respondents do in-house, they were asked what inspection equipment they currently use. All 18 responded, however none of the respondents selected that their inspections were outsourced. The highest selected options, in order, were visual, non-CMM gauges, and CMMs with 3D-CAD models only. The lowest two options receiving votes were CMMs with drawings only and scanning, as seen in Figure 8.

The next question in the survey asked the respondent to rate the level of impact of issues on their business from 1-4, 1 being not an issue and 4 being a serious issue. In between were minor issue (2) and moderate issue (3). Figure 9 shows the mean frequency of the impact of the issues. Below are the issues given to the respondent (1-19) to rate. In Figure 9, these issues are represented by the number associated with them. There were 18 responses to this question.

1. Performing inspection is a bottleneck
2. Performing off line programming for inspection is time consuming
3. Receiving multiple files and/or media formats for as single product
4. 3D-CAD models and associated drawings don't agree
5. 3D-CAD model derivations/translations are problematic
6. Verifying CMM programs is time consuming.
7. 3D-CAD model is not available from customer.
8. Communication with customer is difficult and/or not timely.
9. New designs have producibility issues.
10. Time/volume of report requirements is overwhelming.
11. There are limited design feedback opportunities from supplier to OEM.
12. There is too much variation in production scheduling from OEMs.
13. Data such as 3D-CAD models, drawings, and specifications from customer are not always up to date.
14. Unable to change manufacturing processes due to certification regulations or customer policies.
15. Certification process is sometimes difficult.
16. Obtaining capital is challenging.
17. Ability to hire and retain qualified/skilled workers is problematic.
18. It is expensive to implement Model-based Manufacturing.
19. Help from local, state, and the federal government is either nonexistent or hard to identify.

According to the chart in Figure 9, the issues that impacted companies the greatest (mean above 2.7) were the ability to hire and retain qualified/skilled workers (3.17), performing inspection is a bottleneck (2.89), 3D-CAD models and associated drawings don't agree (2.89), and new designs have producibility issues (2.72). Several issues still had a mean over 2.6 including obtaining capital is a challenge (2.67), it is expensive to implement Model-based Manufacturing (2.67), verifying CMM programs is time-consuming (2.61), data such as 3D-CAD models, drawings, and specifications from customer are not always up to date (2.61). The issues with the lowest impact based on mean were 3D-CAD model derivations/translations are problematic (2.33) and unable to change manufacturing processes due to certification regulations or customer policies (2.33).

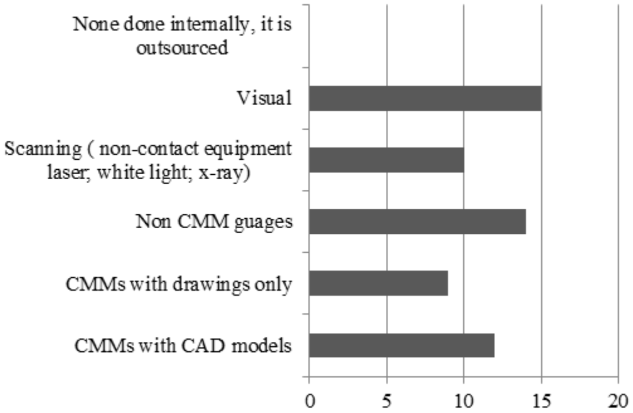


FIGURE 8 - INSPECTION EQUIPMENT USED IN-HOUSE

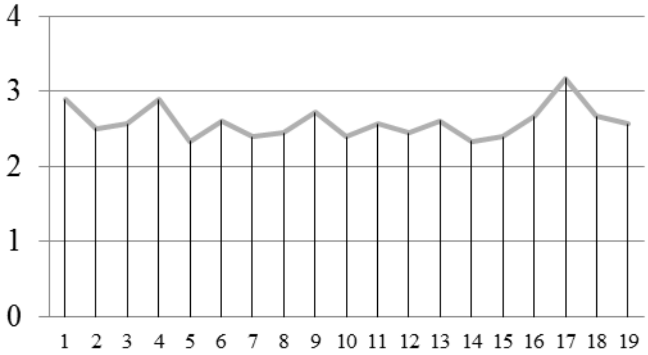


FIGURE 9 - MEAN FREQUENCY OF IMPACT OF ISSUES

Respondents were then asked their current level of capability with using 3D-CAD models as input to their CAM and CMM processes and given three options. The answers they had to choose from were:

- Highly proficient; only minor difficulties
- Somewhat proficient; internal deficiencies still exist
- Currently using drawings and manual input, but have no desire to move to model-based manufacturing

Only one of the respondents claimed they used drawings and had no desire to move to model-based manufacturing. Eleven of the 18 respondents selected somewhat proficient, and six selected highly proficient.

The survey then asked the respondents to select all their manufacturing processes, with only 17 respondents opting to answer. Figure 10 gives a distribution of the selections. Traditional material removal such as cutting, turning, milling, and drilling received every vote, with assembly being the second highest selection.

To wrap up the survey, the respondents were asked what they perceived was the biggest risk for adoption of the Model-based Manufacturing approach as manufacturing and inspection technologies increasingly rely on 3D-digital data. Eighteen respondents were given seven options including other, and capital investment is too large was biggest risk at 28 percent. Figure 11 gives a breakdown of the responses. The responses for other were interoperability.

This breakdown helps give insight into why some companies are not interested yet in moving to MBD. Legacy designs (22%) is almost always an issue because drawings have been used as the main source of information and moving all that data to models can be time consuming and costly. Of the respondents, 22% said there was a lack of business pull, which appears to be that companies do not necessarily see the potential benefits of MBD just yet.

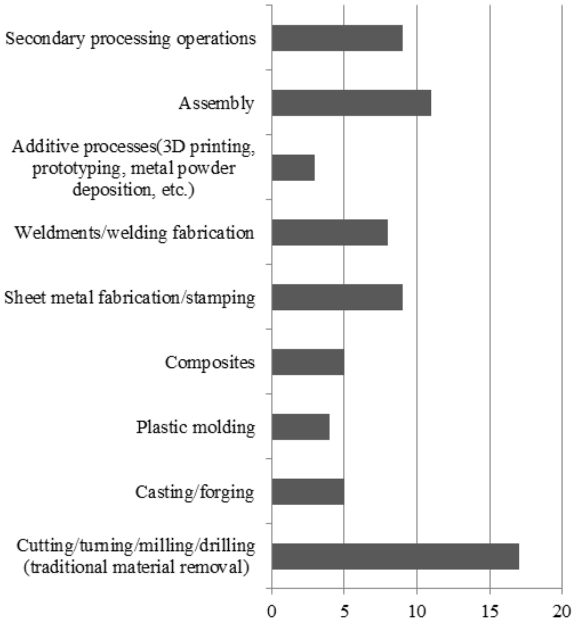


FIGURE 10 - MANUFACTURING PROCESSES USED

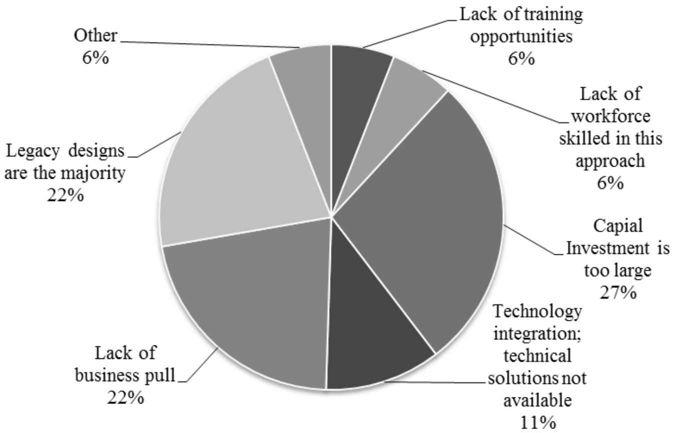


FIGURE 11 - BREAKDOWN OF THE BIGGEST RISKS OF THE ADOPTION OF THE MODEL-BASED MANUFACTURING APPROACH

DISCUSSION AND CONCLUSION

The survey helped give insight to current standing in industry. A fairly wide range of affiliations were represented as well as job positions. A Common Information Model cannot yet be fully defined from these surveys, but critical information has been identified. This information will be used to develop plans for replacement of drawings with 3D-CAD models. These surveys developed the capability of industry's readiness to use models as the master definition and the potential inhibitors of their use.

This paper has supported the need to establish a Common Information Model. A Common Information Model contains the information that is the same from domain specific elements among different aspects of the product's lifecycle. A review of literature was conducted and a survey was analyzed to help give a greater understanding of what information needs to be addressed in the Common Information Model, and where industry stands in terms of implementing MBD. The following are the key results upon which we drew our conclusions:

- A majority of the survey respondents are potentially accepting of the idea of MBD
- Most of the survey respondents already use 3D-CAD models as a source of product data
- Most of the survey respondents still utilize 2D drawings (along with their 3D-CAD models)
- The survey respondents have skepticism and concern about eliminating 2D drawings
- The survey respondents identified several risks when moving from drawings to 3D-CAD models

From our observations of the survey results, we conclude (1) the Common Information Model would need to be workflow specific and (2) more information is needed to establish a Common Information Model for the early phases of the product's lifecycle.

The conclusions from the survey seem to contradict each other; however, they are consistent with what was concluded from the literature review. Industry may be accepting of the idea of MBD, and most already utilize 3D-CAD models for product data, although most still use 2D drawings along with their 3D-CAD models. From these results, it can be concluded industry only accepts the idea of MBD as long as 2D drawings are still used because skepticism remains in completely getting rid of 2D drawings.

While research, such as Hedberg et al. [17], shows MBD can be a major benefit to companies, the survey shows that many industry members have legitimate concerns for only using 3D-CAD models. For example, there are times when using 2D drawings would be easier or make more sense to a company, such as on a shop floor where the company does not have the infrastructure to support 3D-CAD technology. Many respondents felt there was too big of a risk in moving solely to 3D-CAD models from 2D drawings.

While the survey provides evidence that industry is potentially accepting of the idea of MBD and may support the fact that 3D-CAD models can be used as the main source of product data in a production environment, it cannot yet be concluded what information needs to go in to the Common Information Model. The survey helped lay a foundation of knowledge, but more research needs to be done to help understand what specific information goes into the models in the different aspects of the lifecycle.

As of right now, it is difficult to conclude what information is common amongst different models. Based on the results of the surveys, a proposed Common Information Model would need to be workflow specific because of the varying degrees of information in the different workflows. A general Common Information Model would lack enough information to be beneficial to a company's processes.

To establish a Common Information Model, more specific information regarding the workflows is needed. Also, a clearer definition of "common" and "domain specific" will have to be established. A proposed solution would be to have a follow up survey that lists the different elements from this survey and has the respondents "rank" each of them from 1-10, 1 being common and 10 being domain specific. This could help shed light on how the members of industry see the different elements from the lifecycle, which would help further establish the Common Information Model.

ACKNOWLEDGMENTS

This research has been carried out through Purdue University's Product Lifecycle Management Center of Excellence, a part of the Purdue Polytechnic Institute, and in collaboration with the National Institute of Standards and Technology (NIST).

The Engineering Laboratory of the National Institute of Standards and Technology (NIST) supported research reported in this paper under the following grants and/or cooperative agreements:

- 70NANB15H311, Purdue University, "Extending and Evaluating the Model-Based product definition"

The contents of this report do not necessarily reflect the views of NIST. NIST and the authors do not make any warranty, expressed or implied, nor assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in the reports.

This paper may identify certain commercial systems. Such identification does not imply recommendation or endorsement by NIST. Nor does it imply that the products identified are necessarily the best available for the purpose.

REFERENCES

[1] Quintana, V., Rivest, L., Pellerin, R., Venne, F., & Kheddouci, F., 2010, "Will Model-based Definition Replace Engineering Drawings throughout the Product Lifecycle? A Global Perspective from Aerospace Industry," Computers in Industry, **61**(5), pp. 497-508.

[2] Huang, R., Zhang, S., Bai, X., & Xu, C., 2014, "Multi-level Structuralized model-based definition model based on machining features for manufacturing reuse of mechanical parts," The International Journal of Advanced Manufacturing Technology, **75**(5-8), pp. 1035-1048.

[3] ASME Y14.41-2012, 2012, *Digital Product Definition Data Practices*, The American Society of Mechanical Engineers, New York.

[4] ISO 16792, 2006, *Technical Product Documentation– Digital Product Definition Data Practices*, International Organization for Standardization, Geneva, Switzerland.

[5] Camba, J. D., & Contero, M., 2015, "Assessing the Impact of Geometric Design Intent Annotations on Parametric Model Alteration Activities," Computers in Industry, **71**, pp. 35-45.

[6] Fiorentini, X., Rachuri, S., Suh, H., Lee, J., & Sriram, R. D., 2010, "An Analysis of Description Logic Augmented With Domain Rules for the Development of Product Models," Journal of Computing and Information Science in Engineering, **10**(2), Paper No. 021008.

[7] Bouikni, N., Rivest, L., & Desrochers, A., 2008, "A Multiple Views Management System for Concurrent Engineering and PLM," Concurrent Engineering, **16**(1), pp. 61-72.

[8] Bronsvoort, W. F., & Noort, A., 2004, "Multiple-view Feature Modelling for Integral Product Development," Computer-Aided Design, **36**(10), pp. 929-946.

[9] Cera, C. D., Kim, T., Han, J., & Regli, W. C., 2004, "Role-based Viewing Envelopes for Information Protection in

Collaborative Modeling," Computer-Aided Design, **36**(9), pp. 873-886.

[10] Adamski, W., 2010, "Adjustment and Implementation of CAD/CAM Systems Being Used in Polish Aviation Industry," Journal of Machine Engineering, **10**(3), pp. 37-47.

[11] Briggs, C., Brown, G., Siebenaler, D., Faoro, J., & Rowe, S., 2010, "Model Based Definition," AIAA Paper No. 3138.

[12] Andersen, O. A., & Vasilakis, G., 2007, "Building an Ontology of CAD Model Information," *Geometric Modelling, Numerical Simulation, and Optimization*, Springer Berlin Heidelberg, New York, pp. 11-40, Chap. 1.

[13] McKenzie-Veal, D., Hartman, N. W., & Springer, J., 2010, "Implementing Ontology-based Information Sharing in Product Lifecycle Management," 65th Midyear Meeting Proceedings.

[14] Srinivasan, V., 2011, "An Integration Framework for Product Lifecycle Management," Computer-Aided Design, **43**(5), pp. 464-478.

[15] Sudarsan, R., Fenves, S. J., Sriram, R. D., & Wang, F., 2005, "A Product Information Modeling Framework for Product Lifecycle Management," Computer-Aided Design, **37**(13), pp. 1399-1411.

[16] Deelman, E., Gannon, D., Shields, M., & Taylor, I., 2009, "Workflows and e-Science: An Overview of Workflow System Features and Capabilities," Future Generation Computer Systems, **25**(5), pp. 528-540.

[17] Hedberg Jr, T. D., Lubell, J., Fischer, L., Maggiano, L., & Barnard Feeney, A., 2016, "Testing the Digital Thread in Support of Model-Based Manufacturing and Inspection," Journal of Computing and Information Science in Engineering, **16**(2), pp. 1-10. doi:10.1115/1.4032697

10 Volt Automated Direct Comparison of Two Cryocooled Programmable Josephson Voltage Standards

Alain Rüfenacht[1], Yi-hua Tang[2], Anna E. Fox[1], Paul D. Dresselhaus[1], Charles J. Burroughs[1], Robert E. Schwall[1], and Samuel P. Benz[1]

[1] National Institute of Standards and Technology NIST, Boulder, CO 80305, USA

[2] National Institute of Standards and Technology NIST, Gaithersburg, MD 20899, USA

Email: alain.rufenacht@nist.gov

***Abstract* — We have performed direct dc comparisons between two cryocooled 10 V programmable Josephson voltage standards utilizing an automated synchronization scheme for the voltage reversals, which enables the use of a high sensitivity null detector on its 3 µV range by preventing any overload condition. No switches or manual operations are necessary to protect the null detector. Comparing the two systems under various test conditions provides robust verification of ideal system performance, and enables verification of the key components of the uncertainty budget for both the measurement methods and system operations.**

***Index Terms* — Josephson arrays, Precision measurements, Uncertainty, Voltage measurement.**

I. Introduction

The NIST programmable Josephson voltage standard (PJVS) with an output voltage of 10 V has been fully implemented on a cryocooler [1]. Turn-key cryocooled PJVS systems are replacing conventional Josephson voltage standards, not only in national metrology institutes (NMI), but also in primary calibration laboratories (PCL). Direct PJVS to PJVS comparisons [2] are not only becoming prevalent for NMI key comparisons, but are also essential to qualify the performance of PJVS systems disseminated to the PCL. The lowest Type-A uncertainty in direct voltage standard comparisons is generally achieved with the use of an analog null detector [2, 3]. However, the use of an analog detector often demands fastidious manual operations to prevent any overloading during the PJVS polarity reversals required to eliminate the contributions of thermal electromotive forces (EMFs). If the input stage of the analog nanovoltmeter is overloaded, it may take several minutes to completely recover.

This paper presents the first fully automated direct comparison of two cryocooled 10 V PJVS systems. We have developed a synchronization method to simultaneously reverse the polarity of both PJVS systems, which prevents overloading the analog detector, while eliminating the need for a manual low thermal EMF switch to protect the detector input. The main advantage of this method is the ability to automatically acquire longer data sets, thus improving the statistical uncertainty of the comparison and eliminating the risk of improper manual operation that may produce an accidental overload.

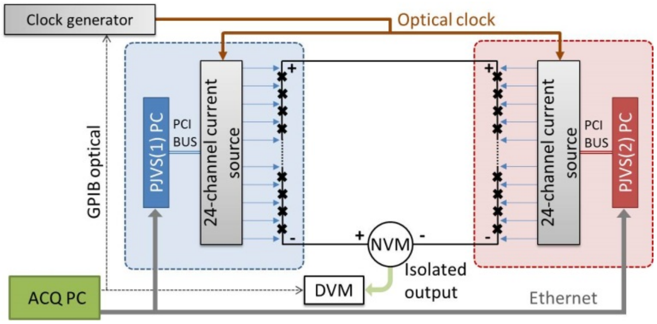


Fig. 1. Block diagram of the automated comparison between the two PJVS systems measured with an analog nanovoltmeter (NVM).

II. Measurement Setup and Synchronization

The measurement setup is presented in Fig. 1. An analog nanovoltmeter (NVM), EM N11[1], was used as a null detector to measure the voltage difference between the two cryocooled voltage standards, PJVS(1) and PJVS(2). The isolated output of the NVM was connected to a digital voltmeter (DVM) for digital readout. The acquisition computer (ACQ PC) controls the amplitude of both PJVS systems by means of an Ethernet connection. The two 24-channel current sources for each PJVS are isolated from ground, and the two microwave generators (not shown) are locked to the same 10 MHz frequency reference (derived from the NIST atomic clock). An arbitrary waveform generator provides two optical clock signals for synchronization, one for each PJVS current bias source. The two PJVS systems are identical, with comparable cable lengths (optical fiber for the clock input, current bias leads, voltage output leads).

The magnitude of the voltage at the input of the NVM, must always remain within the range selected to prevent an overload. Each synchronous change of voltage uses a four-level waveform[2] (Table 1) triggered by four successive clock pulses at 5 kHz (Fig. 2). The waveform is first loaded in the memory of both current sources and is programmed to run for

[1] Certain commercial equipment, instruments, or materials are identified in this report to facilitate understanding. Such identification does not imply recommendation or endorsement by NIST, nor does it imply that the materials or equipment that are identified are necessarily the best available for the purpose.

[2] Minimum waveform size allowed by the current source.

U.S. Government work not protected by U.S. copyright

a single cycle. Once the waveform is completed, the voltage of each PJVS remains at the final voltage level selected.

Table 1. Waveform used to synchronously switch the voltage output polarity of both arrays

Switching mode	Start voltage	Waveform (4 levels)			
		#1	#2	#3	#4 (end)
A (start)	**0 V**	0 V	0 V	10 V	**10 V**
B (+ → -)	**10 V**	0 V	0 V	-10 V	**-10 V**
C (- → +)	**-10 V**	0 V	0 V	10 V	**10 V**
D (end)	**10 V**	0 V	0 V	0 V	**0 V**

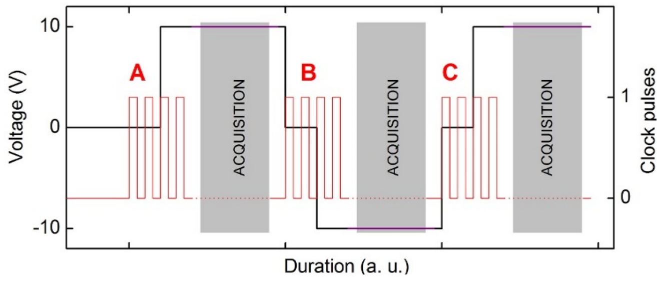


Fig. 2. Schematic of the waveform used to perform the synchronous switching between voltages, (A: start, B: from +10 V to -10 V, and C: from -10 V to 10 V). The four clock pulses are shown in red. The data acquisition occurs once both PJVS output voltages are fully settled (gray area).

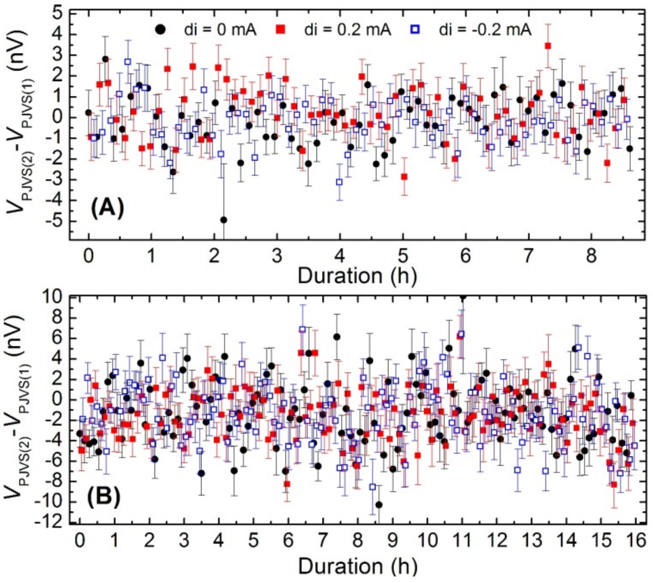


Fig. 3. Comparison results with (A) both systems floating from ground, and (B) with the low input of the NVM connected to earth ground.

III. Results

Figure 3 shows the results of two multi-hour automated comparisons at 10 V. Each value reported is calculated with a linear fit based on four polarity reversal sets "+-+-" in order to remove the contributions of thermal EMFs. A polarity set consists of 15 DVM readings at 10 power line cycles. The Type-A uncertainty shown (error bar, $k = 1$) is extracted from the fit residuals [4]. No overload is observed during the polarity reversals with the NVM set to the 3 μV range and the filter set to the maximal bandwidth (position 1), which confirms that the synchronization method is successful. To minimize potential error due to dielectric absorption time, the acquisition of each set starts 40 s after switching the voltage polarity. The data in both plots of Fig. 3 utilize the applied dither current technique [2], which confirms that both PJVS systems maintain a sufficient current margin when connected in series to the NVM throughout the full measurement time. The reported data are not corrected for the gain error of the NVM, since the measured relative correction is less than 5 pV/nV and is well below the noise floor of the measurement.

The result extracted from Fig. 3A shows excellent agreement between the two PJVS systems of $V_{\text{PJVS(2)}}$ - $V_{\text{PJVS(1)}}$ = (-0.05 ± 1.22) nV, where the uncertainty is the standard deviation ($k = 1$). Additional analysis of the 1/f noise of the detector will be required to determine the standard deviation of the mean. However, when the low input of the NVM is connected to ground (Fig. 3B), the final result is $V_{\text{PJVS(2)}}$ - $V_{\text{PJVS(1)}}$ = (-1.26 ± 3.11) nV. Grounding the circuit modifies the leakage current distribution, which affects the result of the comparison and also slightly increases the noise of the measurement. Due to the complex distribution of the leakage current in PJVS systems, additional measurements are required to understand and evaluate the uncertainty contributions related to leakage.

IV. Conclusion

We have performed automated comparisons between two cryocooled PJVS systems at 10 V dc. Synchronization of the two systems when switching between output levels enables the use of a high sensitivity null detector with a ±3 μV input range. No switches or manual operator tasks are required in these measurements, which minimizes wiring connections. In the final paper on this work, we will present a detailed uncertainty budget including further investigation of potential Type-B contributions.

References

[1] A. Rüfenacht, *et al.*, "Cryocooled 10 V Programmable Josephson Voltage Standard," *IEEE Trans. Instrum. Meas.*, vol. 64, no. 6, pp. 1477–1482, Jun. 2015.

[2] S. Solve, *et al.*, "Direct comparison of two NIST PJVS systems at 10 V," *Metrologia*, vol. 50, no. 5, pp. 441–451, 2013.

[3] S. Djordjevic, *et al.*, "Direct comparison between a programmable and a conventional Josephson voltage standard at the level of 10V," *Metrologia*, vol. 45, pp. 429–35, 2008.

[4] C. A. Hamilton, *et al.*, "A compact transportable Josephson voltage standard," *IEEE Trans. Instrum. Meas.*, vol. 46, no. 2, pp. 237–241, Apr. 1997.

Direct Comparison of a Pulse-driven Josephson Arbitrary Waveform Synthesizer and a Programmable Josephson Voltage Standard at 1 Volt

Alain Rüfenacht, Nathan E. Flowers-Jacobs, Anna E. Fox, Charles J. Burroughs, Paul D. Dresselhaus, and Samuel P. Benz

National Institute of Standards and Technology NIST, Boulder, CO 80305, USA
Email: alain.rufenacht@nist.gov

***Abstract* — We have performed direct ac comparisons between two types of quantum voltage standards, a pulse-driven Josephson arbitrary waveform synthesizer and a programmable Josephson voltage standard, at 1 V rms amplitude and a frequency of 100 Hz. The system architectures for these two Josephson technologies are quite different. However, in the range where their capabilities overlap, they should produce identical results. This comparison under various test conditions is a powerful method for verifying ideal performance of the systems, and exploring a number of potential systematic errors in both measurement methods and system operations.**

***Index Terms* —, Josephson arrays, Signal sampling, Standards, Voltage Measurement.**

I. Introduction

Programmable Josephson voltage standards (PJVS) are capable of generating stepwise-approximated reference waveforms with frequencies ranging from sub-hertz to a few kilohertz. Such waveforms, when combined with a sampling voltmeter and the differential sampling method, have been used to determine the root-mean-square (rms) output voltage of a commercially available high spectral-purity voltage source [1]. Recent improvements in superconductive circuit design and pulse generator electronics for the Josephson arbitrary waveform synthesizer (JAWS) have enabled 1 V rms output voltages and have extended the low end of the waveform frequency range down to 1 Hz [2]. With the JAWS and PJVS operating ranges now significantly overlapping, both indirect [3] and direct [4] comparisons between these two types of quantum voltage standards are possible.

Taking advantage of the intrinsic stability of the JAWS and the PJVS, direct comparison is an ideal tool to verify the parameter range where quantum accuracy is achieved in both systems. Subsequently, we can search for potential systematic errors associated with both the quantum voltage standards and the comparison technique. This paper presents initial results at 1 V and discusses the challenges associated with directly comparing the two quantum voltage standards.

II. Differential Sampling

Both the JAWS and PJVS systems were operated in liquid helium with waveforms at rms amplitudes of 1 V and a frequency of 100 Hz. A commercially available digitizer measures the differential voltage between the low-voltage output lead of each system. The digitizer is battery powered, and therefore floating. All the instruments are locked to the same 10 MHz clock reference (NIST primary frequency standard). Synchronization between the two waveforms and the digitizer is achieved with optically coupled trigger signals generated by the PJVS electronics and connected to both the JAWS pulse generator and the digitizer. The relative phase between the two waveforms is adjusted by rotating the pattern of the JAWS waveform in order to minimize the differential voltage. Prior to every data acquisition, the average gain error of the digitizer is measured with a 60 mV peak amplitude PJVS waveform. The duration of each PJVS level is set to 125 µs ($N = 80$ levels/period and 100 Hz). We acquire 100 periods of the differential voltage with a sampling frequency of 10 MHz, average, and apply the previously mentioned gain correction for the digitizer [5]. The first 30 µs and last 10 µs of each PJVS level are discarded to remove the PJVS transients and the oscillations due to the finite impulse response filter of the digitizer. The JAWS sine wave is reconstructed by adding the corrected differential voltages to the nominal PJVS levels, and the fundamental of the JAWS sine wave ($V_{\mathrm{MEAS}}^{(\mathrm{PJVS})}$) is extracted with a sine-fit. The deviation from the nominal value V_{JAWS}=1 V is given by $\Delta V = V_{\mathrm{MEAS}}^{(\mathrm{PJVS})} - V_{\mathrm{JAWS}}$.

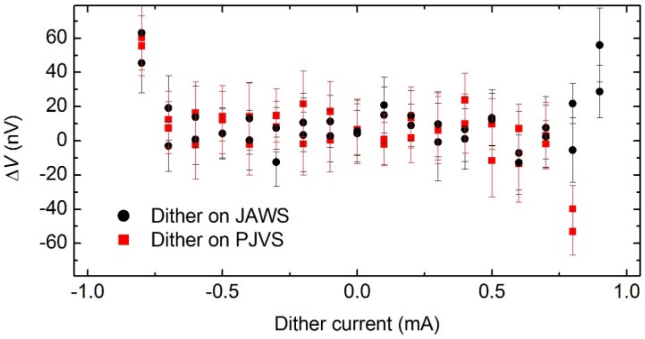


Fig. 1. Measured dither current flat-spot of the PJVS and JAWS systems with their outputs connected in series.

III. Measurements

Each data point represented in the manuscript is the mean value of 25 consecutive measurements. The error bars represent the Type-A uncertainty ($k = 2$). Measurements were repeated twice to show the repeatability. Figure 1 shows the effect of a dc current offset applied to the PJVS array ("S" shape, red squares) and the JAWS array ("U" shape, black

U.S. Government work not protected by U.S. copyright

Rufenacht, Alain; Flowers-Jacobs, Nathan; Fox, Anna; Burroughs, Charles; Dresselhaus, Paul; Benz, Samuel. SP-848
"Direct comparison of a Pulse-driven Josephson Arbitrary Waveform Synthesizer and a Programmable Josephson Voltage Standard at 1 Volt."
Paper presented at the CPEM 2016 Conference, Ottawa, Canada, Jul 10-Jul 15, 2016.

dots). Note that with the JAWS-PJVS differential configuration the amplitude resolution obtained is a few nanovolts, which is a 20 times greater sensitivity than attained with previous methods (i.e., using the digitizer directly with the JAWS or PJVS).

Both measurements show that $\mathit{\Delta}$V is constant over a range of offset detuning, namely "flat-spots" with magnitudes 1.4 mA (PJVS) and 1.5 mA (JAWS). Note the excellent agreement between PJVS and JAWS amplitude. ΔV is on the order of 10 nV over the full flat-spot range, corresponding to a measured relative difference of less than a few parts in 10^8.

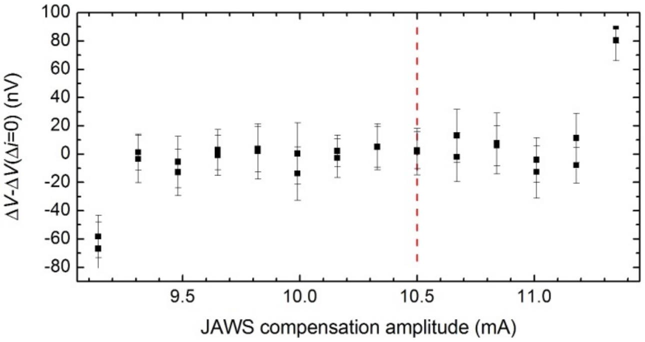


Fig. 2. Flat-spot measurement of ΔV vs. the JAWS compensation signal amplitude (repeated twice). The flat-spot boundaries correspond to a compensation amplitude variation of -1 .2 mA to +0.7 mA relative to 10.5 mA ($\Delta i = 0$), the setting selected where the operating margin is maximum.

Direct comparison between the JAWS and the PJVS is a high-resolution diagnostic tool for measuring the operating range over which the various bias parameters retain quantum-accurate outputs of the JAWS and PJVS systems. For example, Fig. 2 presents the flat-spot obtained as a function of the JAWS compensation amplitude [2]. For clarity, the data on the y-axis are expressed as a relative quantity to highlight the effect of the dithered parameter. We plan to measure flat-spots for all of the JAWS and PJVS bias parameters.

Figure 3 presents the effect of detuning the PJVS amplitude from the ideal 1 V that matches the JAWS amplitude, thus forcing the digitizer to measure larger difference voltages. There is a small slope in Fig. 3 indicating that the measured error is proportional to ΔV_{PJVS}. We applied a simple gain correction on the digitizer measured data (typically of the order of 6 parts in 10^5), but a small, non-negligible, systematic error on the determination of ΔV remains. Further investigations on the non-linearity of the digitizer and its impact on ΔV are required in order to minimize this error.

IV. Discussion

The results presented in Fig. 3 emphasize the critical importance of searching for and evaluating all potential systematic effects related to voltage differences (ΔV). Among other potential errors, leakage currents are a critical component of the uncertainty budget that must be evaluated. Unlike PJVS to PJVS comparisons, where the various leakage resistances to ground are of primary importance, additional leakage effects due to the stray capacitances to ground are likely to be important when comparing ac voltage waveforms. We plan to perform the JAWS-PJVS comparison with various earth grounding configurations that may provide additional information to evaluate the Type-B uncertainty associated with leakage currents. Additionally, the voltage error contribution due to the on-chip inductors also needs to be evaluated as function of the waveform frequency.

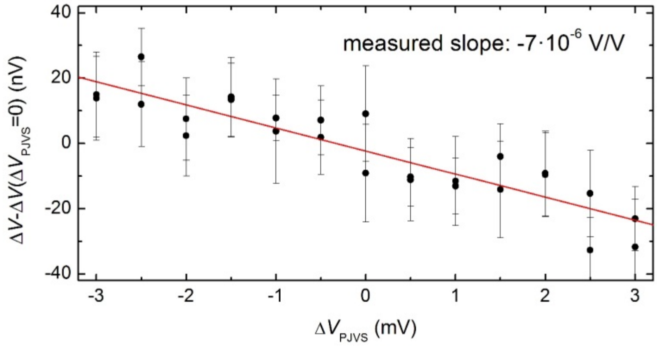


Fig. 3. Measured linear dependence of the relative JAWS rms amplitude as a function of PJVS amplitude variation $\Delta V_{\mathrm{PJVS}} = V_{\mathrm{PJVS}} - 1$ V (repeated twice).

V. Conclusion

The agreement between the NIST JAWS and PJVS systems at 1 V rms and 100 Hz is presently measured to be a few parts in 10^8. The reported offset current margins of 1.4 mA or more for both systems confirms that both Josephson standards retain large operating margins when connected in series. We will continue our work on JAWS-PJVS comparisons with additional measurements, including a detailed analysis of potential systematic errors associated with both the quantum voltage standards and the measurement method so as to present a complete uncertainty budget.

References

[1] A. Rüfenacht, *et al.*, "Differential sampling measurement of a 7 V rms sine wave and a programmable Josephson voltage standard," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 6, pp809-815, June 2013.

[2] S. P. Benz, *et al.*, "Performance Improvements for the NIST 1 V Josephson Arbitrary Waveform Synthesizer," *IEEE Trans. Appl. Supercond.*, vol. 25, no. 3, pp. 1400105-6, June 2015.

[3] B. Jeanneret*, et al.*, "High precision comparison between a programmable and a pulse-driven Josephson voltage standard," *Metrologia* 48, pp. 311–316, 2011.

[4] R. Behr, *et al.*, "Direct comparison of a 1 V Josephson arbitrary waveform synthesizer and an ac quantum voltmeter," *Metrologia* 52, pp. 528–537, 2015.

[5] C. J. Burroughs, *et al.*, "Method for ensuring accurate ac waveforms with programmable Josephson voltage standards," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 6, pp. 1627-1633, June 2013.

Simultaneous Double Waveform Synthesis with a Single Programmable Josephson Voltage Standard

Alain Rüfenacht[1], Anna E. Fox[1], Paul D. Dresselhaus[1], Charles J. Burroughs[1], Samuel P. Benz[1], Bryan C. Waltrip[2], and Thomas L. Nelson[2]

[1] National Institute of Standards and Technology NIST, Boulder, CO 80305, USA

[2] National Institute of Standards and Technology NIST, Gaithersburg, MD 20899, USA

Email: alain.rufenacht@nist.gov

***Abstract* — We have recently demonstrated new 2 V PJVS devices configured with two voltage outputs and two sets of least significant bits in order to simultaneously generate two independent stepwise output waveforms. This development improves upon our previous alternating dual waveform method in that the two voltage waveforms can now be measured simultaneously, and the sampler overload condition that existed in the previous configuration has been eliminated. Applications such as the NIST Quantum Watt for ac power calibrations will benefit from these developments through reduced measurement uncertainties and improved flexibility.**

***Index Terms* — Josephson arrays, Signal sampling, Standards, Power Measurement, Voltage Measurement.**

I. Introduction

Programmable Josephson voltage standards (PJVS) have improved continuously since 1995 [1]. Besides dc voltage metrology applications in which the 10 V PJVS systems are commonly used, PJVS systems with lower output voltage (1 V or 2 V) are implemented in other applications such as the electronic kilogram programs and in low-frequency ac electric power programs, such as the NIST Quantum Watt [2].

The Quantum Watt requires two independent low harmonic distortion voltage sources with typical rms amplitudes of 1.2 V and 0.5 V. These two reference sources are utilized to measure, respectively, the voltage and the current components of electric power. Presently, the rms value of each source is alternately measured using the differential sampling method and a multi-period reference waveform generated by a single PJVS [3].

This paper presents a new method to simultaneously synthesize two voltage waveforms from a single 2 V PJVS circuit recently developed at NIST. The advantage of this method is the new ability to simultaneously measure the voltage and current waveforms with a single PJVS system, which reduces both the complexity and operating costs of the Quantum Watt.

II. 2 V PJVS Array

We have developed a 2 V PJVS superconducting integrated circuit containing 61 204 Josephson junctions (JJs) that are capable of generating a maximum dc output voltage of ±2.278 V when biased at a microwave frequency of 18 GHz (Fig. 1). The circuit is equipped with two full and identical sets of least significant bits (LSBs), one on each extremity of the chip, that are each subdivided in a ternary sequence. The smallest LSB contains four JJs in a single segment, which is made from a pair of double stack $Nb/Nb_xSi_{1-x}/Nb/Nb_xSi_{1-x}/Nb$ junctions. The mirrored distribution of the subarrays across the chip allows for a perfect 0 V output during dither current flat-spot measurements when the symmetric matching subarrays are biased alternately on the $n = \pm 1$ steps. These circuits are capable of operating over a wide microwave frequency range from 15 GHz to 21 GHz.

An extra common voltage tap was added to this new 2 V PJVS circuit to allow the top and bottom array subsections to produce independent voltage outputs. The dc-current-bias electronics developed for the NIST 10 V PJVS, which contains 24 digital-to-analog converter (DAC) voltage sources each with a 112 Ω bias resistor, is fully compatible with the 20 subarrays of the new 2 V PJVS circuit. Figure 2 shows a flat-spot width of 1.75 mA measured with nanovolt resolution.

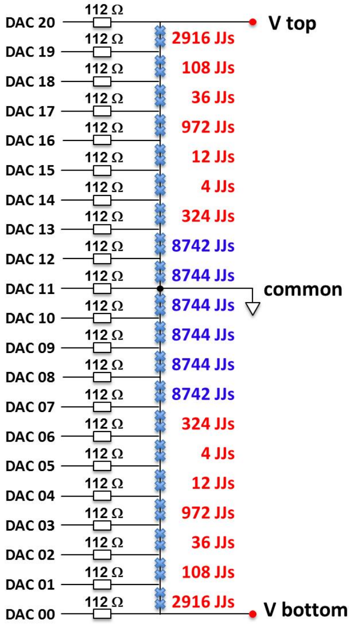


Fig. 1. Block diagram of the 2 V PJVS circuit, illustrating the two sets of LSBs (number of JJs in red), the current bias leads (left side), and the voltage output taps (right side).

U.S. Government work not protected by U.S. copyright

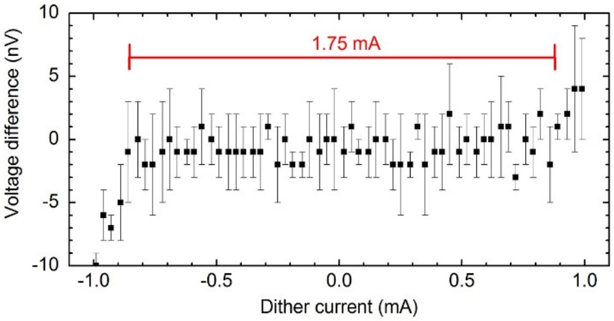


Fig. 2. Dither current flat-spot measurement performed with the first half of the 2 V subarrays biased on the $n = +1$ step and the second half biased on the $n = -1$ step. The error bars represent the standard deviation (k=1) of four measurements.

III. Double Waveform Synthesis

In order to generate two independent voltage outputs from a single chip, the array circuit is divided into two sections separated by the common tap (Fig. 1). The bottom and top sections, respectively, contain 39 346 JJs and 21 858 JJs. When biased with a microwave frequency of 20.86 GHz, the peak voltages for each section are $V_{\text{bottom}} = 1.697$ V and $V_{\text{top}} = 0.943$ V. These values enable the PJVS to simultaneously generate the two stepwise-approximated reference sinewaves with rms amplitudes of 1.2 V and 0.5 V that are required for the NIST Quantum Watt.

To implement this double voltage waveform synthesis, some simple hardware modifications were made to the existing NIST PJVS system. Two additional twisted pair voltage outputs run from the chip to room temperature, and their corresponding two coaxial output connectors (for V_{top} and V_{bottom}) are mounted on the cryoprobe. The connector outer shields share the on-chip common node.

The software was modified to generate arbitrary waveforms for the two outputs. At each step in the waveform sequence the array common node adjacent to DAC 11 (denoted by the black dot in Fig. 1) is kept at a potential of 0 V, which limits the capacitive loading effect of the bias electronics power supply. The bias electronics are fully isolated from earth ground, so the user can choose whether or not to ground the common node for a given application. Since a single microwave source is used to bias both sections of the array, fine adjustment of the voltage by slightly detuning the microwave frequency can only be performed relative to a single output. Both waveforms are loaded simultaneously and share the same clock signal. Relative phase adjustment between the two waveforms is achieved by adjusting the waveform data with a resolution of 172.5 μV (4 JJs), as shown in Fig. 3.

IV. Application to the Quantum Watt

As presently implemented in the Quantum Watt, the PJVS reference waveform alternates between the two waveform amplitudes every 16 to 20 periods [3], due to the finite 2048 sample size of the DAC biases. As a result, the acquisition time of the differential voltage is reduced, increasing the Type-A uncertainty on the signal of interest [4]. Furthermore, each sampling voltmeter is overloaded half of the time, requiring some time (typically one period of the signal of interest) to recover [3]. The new circuit, with dual waveform synthesized output signals eliminates these two limitations. Our next step will be to integrate the simultaneous double PJVS reference waveforms into the Quantum Watt measurement apparatus, utilizing two sinusoidal reference voltage sources and two sampling voltmeters.

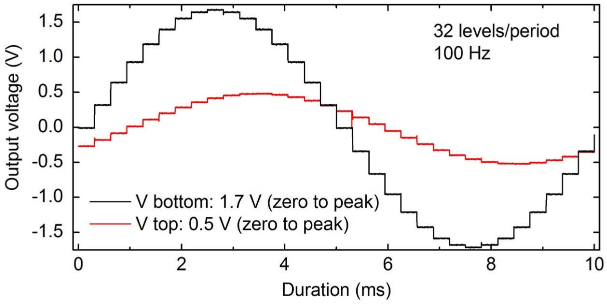


Fig. 3. Example of simultaneously-measured oscilloscope traces of the PJVS output voltages V_{top} and V_{bottom}. The two stepwise-approximated PJVS waveforms shown have 32 levels each, and a frequency of 100 Hz. The relative phase difference between the two waveforms is software selectable, and in this example is 30 degrees.

V. Conclusion

The recent development of a 2 V PJVS circuit with dual voltage outputs, including two sets of LSBs, allows a single PJVS system to simultaneously generate two different output voltages. The NIST electric power standard will benefit from this new capability and measurement method, with the advantage of increasing the performance of the present differential sampling approach with minimal hardware modification. This method opens the door to new metrology applications that require two voltages, and avoids the complication and cost of two independent PJVS systems.

References

[1] S. P. Benz, "Superconductor–normal metal–superconductor junctions for programmable voltage standard," *Appl. Phys. Lett.*, vol. 67, pp. 2714–2716, 1995.

[2] B. C. Waltrip, *et al.*, "AC power standard using a programmable Josephson voltage standard," *IEEE Trans. Instrum. Meas.*, vol. 58, no. 4, pp. 1041–1048, Apr. 2009.

[3] A. Rüfenacht, *et al.*, "Precision differential sampling measurements of low-frequency voltages synthesized with an AC programmable Josephson voltage standard," *IEEE Trans. Instrum. Meas.*, vol. 58, no. 4, pp. 809–815, Apr. 2009.

[4] A. Rüfenacht, *et al.*, "Differential sampling measurement of a 7 V RMS sine wave with a programmable Josephson voltage Standard," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 6, pp. 1587–1593, June 2013.

Rufenacht, Alain; Fox, Anna; Dresselhaus, Paul; Burroughs, Charles; Benz, Samuel; Waltrip, Bryan; Nelson, Thomas.
"Simultaneous Double Waveform Synthesis with a Single Programmable Josephson Voltage Standard."
Paper presented at the CPEM 2016 Conference, Ottawa, Canada, Jul 10-Jul 15, 2016.

Proceedings of the ASME 2015 International Mechanical Engineering Congress & Exposition
IMECE2015
November 13-19, 2015, Houston, Texas

IMECE2015-50654

A CONSTRAINED L_2 BASED ALGORITHM FOR STANDARDIZED PLANAR DATUM ESTABLISHMENT

Craig M Shakarji
Physical Measurement Laboratory
National Institute of Standards and Technology
Gaithersburg, Maryland 20899
craig.shakarji@nist.gov

Vijay Srinivasan
Engineering Laboratory
National Institute of Standards and Technology
Gaithersburg, Maryland 20899
vijay.srinivasan@nist.gov

ABSTRACT

For years (decades, in fact) a definition for datum planes has been sought by ASME and ISO standards writers that combines the contacting nature of traditional surface plate mating with a means of balancing rocking conditions when there is a centrally positioned extreme point or edge on the datum feature. This paper describes a completely self-balancing method for datum plane establishment that matches traditional surface plate mating while automatically stabilizing rocker conditions. The method is based on a constrained L_2 (L2) minimization, which, when seen mathematically, elegantly combines the desirable contact properties of the constrained L_1 (L1) minimization with the stable properties of the unconstrained least-squares and does so in a manner that avoids the drawbacks of either of those two definitions. The definition is shown along with proofs of a mathematical development of an algorithm that relies on a strategically chosen singular value decomposition that allows for an elegant, robust solution. Concise code is included for the reader for actual use as well as to full clarify all the algorithmic details.

Testing has shown the definition defined here does indeed provide attractive balancing of full contact with rocker stability, leading to guarded optimism on the part of the key standards committees as an attractive default definition. Since both the ISO and ASME standardization efforts are actively working to establish default datum plane definitions, the timing of such a rigorously documented study is opportune.

1. BACKGROUND AND INTRODUCTION

In the world of Geometric Dimensioning and Tolerancing (GD&T), datums are used extensively to locate and orient tolerance zones [1-7]. Datum planes in particular are common and are established by mating planes to imperfect datum features on parts during inspection [3] (see Fig. 1). Distances and orientations on drawings and three-dimensional models are established from these datum planes, relative to which tolerance zones are located and oriented. In many cases there is a need for more than one datum plane. In fact a full Cartesian coordinate system in three dimensions is often established using datums. Datum planes, in particular, are widely used for this. The importance and prevalence of datum planes in specifications are given in greater detail in [8] and will not be revisited in this paper.

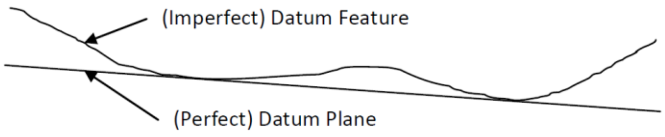


Fig. 1. Deriving a datum plane from a datum feature.

Given that datum planes are ubiquitous, it might be surprising that—short of standardization—there are several different yet reasonable approaches by which a datum plane can be established from a datum feature [9]. Furthermore, the International Organization for Standardization (ISO) and the American Society for Mechanical Engineering (ASME) are actively working to establish default datum plane definitions.[1]

[1] The constrained L_2 planar datum definition, as described in this paper, has been adopted as the default planar datum definition for by ISO for the Draft International Standard ballot to take place in 2015 for the revision of ISO 5459

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

Consequently, the timing of this paper is opportune, since we seek to demonstrate an algorithm that naturally combines a correspondence to physical, surface plate mating with automatic balancing in the case of rockers.

Till now the ASME definitions (ASME Y14.5, Y14.5.1) have employed a complex "candidate" datum system, which they now desire to replace or supplement with a default, unambiguously defined planar datum. The ISO working group is also seeking to improve its default planar datum definition in its emerging replacement of the ISO 5459 standard. The ISO definition (ISO 5459) had, since 1982, relied on non-rigorous language that implies using the full contact of a surface plate with balancing in the case of rocking conditions (and an intermediate "improvement" has its own issues). Both standards groups seek a mathematical definition that makes sense in ordinary cases of surface plate mating but one that also balances rocking conditions. The purpose of this paper is to document a new and advantageous definition and algorithm for establishing a datum plane from a datum feature—one that is appropriate for national and international standard definitions.

In Section 2 of this paper, we define what the L_2 norm is in the context of datum planes. Section 3 gives details of another planar datum definition based on a constrained L_1 norm that will give the appropriate context to understand the benefit of the constrained L_2 solution. Section 4 details the constrained L_2 algorithm and gives mathematical details that show how it is actually a combination of traditional least-squares fitting and the constrained L_1 datum. That section also gives mathematical means for an efficient algorithm. Section 5 is an important part of the paper, as it answers why L_2 the constrained datum definition is appealing in that it automatically gives the desired result of a full contact or balancing solution. Section 6 gives our conclusions. Matlab code for the 2D case is included in the appendix for any readers who wish to independently examine the effects of the algorithm on various data sets.

2. L_2 NORM DEFINED IN THE CONTEXT OF DATUM PLANES

First, we describe what is meant by a constrained L_2 fit in our context.[2] To fit a one-sided L_2 plane to a surface patch in space, we pose the following optimization problem (with reference to Fig. 2): Given a bounded surface S, and a direction $\boldsymbol{a}^*$ (that points into the material), find the plane P that minimizes $\int_S |d^2(\boldsymbol{p},P)|ds$, subject to the constraint that P lies entirely to one side (as determined by $\boldsymbol{a}^*$) of the surface S.

Here $d(\boldsymbol{p},P)$ denotes the signed perpendicular (to P) distance of a point $\boldsymbol{p}$ on surface patch S from the plane P that will be fitted. We note that $\int_S ds$ is the area of the surface patch. If the surface consists of several patches, then the integrals can be evaluated over each patch and then summed.

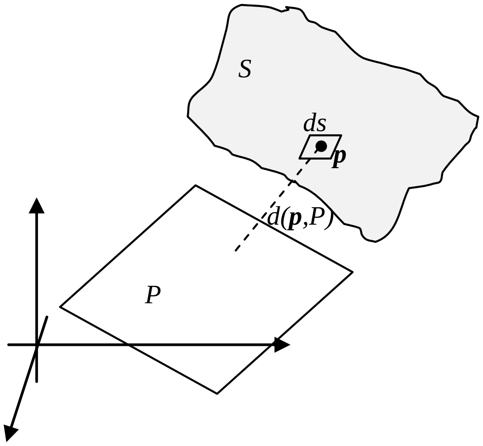


Fig. 2. Fitting a plane to a surface patch.

The objective function cannot, in general, be evaluated in closed form. So we resort to numerical integration over the surface S. We can sample points on a surface patch after dividing up the patch into discrete areas ΔA_i and approximate the objective function as

$$\int_S d^2(\boldsymbol{p},P)ds \approx \sum_{i=1}^{N} d^2(\boldsymbol{p}_i,P)(\Delta A_i)\,, \tag{1}$$

where $\boldsymbol{p}_i$ are the N sampled points, one in each subdivision. Thus we are led to minimizing $\sum_{i=1}^{N}[|d(\boldsymbol{p}_i,P)|\cdot\Delta A_i\,]$ over the parameters of the plane P, where ΔA_i's are treated as the weights.

The distance from a point $\boldsymbol{p}$ to a plane P defined by a point on the plane, $\boldsymbol{p_0}$, and the unit normal to the plane, $\boldsymbol{a}$, is

$$d(\boldsymbol{p},P) = \boldsymbol{a}\cdot(\boldsymbol{p}-\boldsymbol{p_0}).$$

The two-dimensional case is a readily-apparent restriction from the three-dimensional case shown above.

3. A BRIEF LOOK AT THE CONSTRAINED L1 MINIMIZATION DATUM PLANE DEFINITION

Before examining the advantageous properties of the constrained L_2, it is helpful to understand the constrained L_1 datum plane definition—both its advantages and disadvantages. Doing so will highlight how the new, constrained L_2 definition largely keeps the advantages of the constrained L_1, along with elegantly removing the issues with the constrained L_1.

on datums. Thus it is likely that this datum plane definition will be adopted for worldwide use.

[2] The L_2 norm is also known as a least-squares norm. However, in this paper, in order to avoid confusion, the datum definition we propose is consistently called the constrained L_2 datum. It is not called a constrained least-squares plane (though correct) in order to emphasize that this is different than the normal least-squares plane and also different from a shifted least-squares plane.

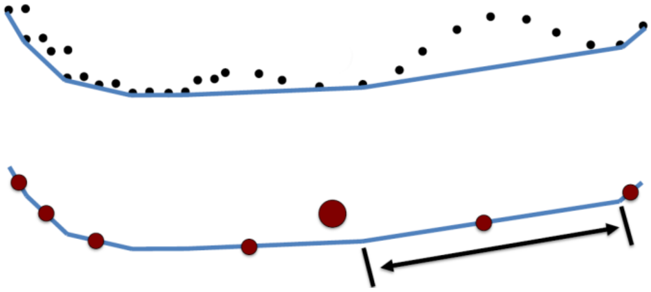
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

In an earlier paper [8] and then improved in [10], we presented the theory and algorithms for datum plane establishment using a constrained minimization search based on the L_1 norm. In short, the algorithm worked as follows: Given a surface (or set of sampled points), the datum plane was defined as the plane that (1) is constrained to lie on the nonmaterial side of the surface (or points), and (2) minimizes the integral (or sum) of absolute distances between the plane and the surface (or points). We showed that finding such a plane actually turns out to be quite simple, since we proved that it is equivalent to finding the plane that minimizes the distance between the centroid of the surface (or of the weighted points) and the plane. This simplification led to efficient algorithms (and code provided) for the primary and secondary planar datums (the tertiary case being trivial).

The reader is encouraged to fill in details as desired from the earlier paper itself [10], but we give a summary of the constrained L_1 algorithm as follows:

1) Given a set of points sampled on a surface, compute the lower convex envelope of those points. This surface is the part of the convex hull of those points that lies to the outside of the material. The constrained L_1 definition will now be applied to this surface (as opposed to the points)
2) Compute the centroid of the surface as the weighted combination of the centroids of the triangles making up the convex surface. In 2D, the centroid of the convex, piecewise linear curve would be computed as the weighted combination of the centroids (midpoints) of the line segments that it is comprised of. The weights are the relative areas of the triangles (or relative lengths of the line segments in 2D, one such length shown in fig. 3, middle picture).
3) Find the plane containing a triangular facet of the convex hull closest to the computed centroid (or, in 2D, find the line containing a line segment of the curve closest to the centroid).

Figure 3 shows these three steps in a 2D case.



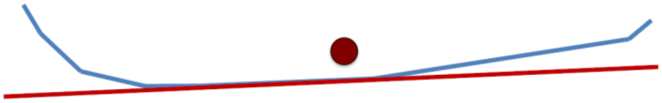


Fig. 3. The three main steps of computing the constrained L_1 datum plane, given a discrete set of points.

Theorems were proved in [10] that showed that the algorithm summarized above is an efficient means of exactly obtaining the constrained L_1 datum plane. Some of the appealing properties of this method are:

1) It mimics the contact achieved by the effect of gravity, if the surface were placed onto a mathematically perfect, horizontal plane.
2) In a 3-2-1 datum reference frame, the primary datum plane always contacts three data points (minimum) and the secondary, always two minimum. This is in the context of discrete, sampled points.
3) The method works well even for non-uniformly sampled data without needing any weights to be provided for the points or any part information.
4) The method yields pleasing results for several example cases studied.

Other advantages are given in [10], but these should suffice for our needs here. In summary, the appeal of the constrained L_1 definition is how closely it mimics many uniform-thickness, real parts sitting on surface plates under the influence of gravity.

However, common practice with a surface plate also employs balancing rocker conditions as shown in fig. 4.

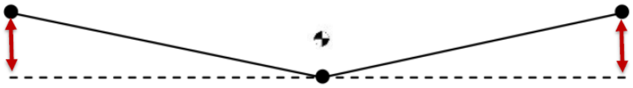


Fig. 4. A planar datum feature of a wedge shape being stabilized to avoid rocking, thus giving the dashed line shown as the datum.

If the constrained L_1 definition were applied to the wedge shape shown in fig. 4, the datum plane would lie coincident with one side or the other of the datum feature. This drawback manifests itself in a few important ways. First, if the part were convex (bowl shaped) and sampled with five points (one in each corner and one in the middle) then the effect would be that of an upside-down pyramid, and the constrained L_1 plane would coincide with one of its triangular faces. In a symmetric case, the choice of which triangular face would be chosen would depend on something as little as measurement error during the time of inspection.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

Another case to consider is a 3D concave datum feature, where a rectangular feature has four low spots, one at each corner. In this case, the part would naturally sit on a horizontal plane like a four-legged chair. That is, it would rest along one diagonal (contacting two opposite corners) and rock between contacting either of the two corners off that diagonal. Here again, the desire among many in the standards communities is to balance that rock, a feature the constrained L_1 definition does not employ.

It does little good to seek to remedy the various rocking situations described by simply stating in words that the constrained L_1 definition holds except in rocking situations, where the rock should be balanced. This is insufficient (1) due to the lack of rigor in defining a rocking condition and (2) due to the lack of rigor in defining how the rock should be balanced. But even if crisp definitions are added to the above words, there would still be discontinuities at the thresholds of rocking/non-rocking states that could lead to instability in the resulting datum plane from one measurement to the next.

In contrast to the problems just described with the constrained L_1 datum definition, it is well known that the traditional least-squares fitting plane is a smoothly varying, stable association to a planar feature.[3] We will show that the constrained L_2 takes the best of both worlds. It exactly matches the L_1 solution when there is not a rocker condition and also (naturally and automatically) balances rocker conditions smoothly (like traditional least-squares) without any special “if” statements employed to do so.

4. THE CONSTRAINED L_2 DEFINTION AND EFFICIENT ALGORITHM

As in the constrained L_1 defintion above, the proposed constrained L_2 datum plane definition first forms the lower convex surface of the datum feature and then finds the plane that minimizes the sum-of-squares (or integral, in the continuous case) of the distances from the plane to that convex surface.

The reasons for forming the convex envelope first are given in detail in [10], but are summarized by these three points: (1) it represents the actual interaction of a plane with the feature (if one rocks a datum feature on a perfect plane, the plane never contacts the concave sections), (2) it prevents the need for weights or part information when given discrete data points, since the convex envelope allows appropriate weighting to be included in the algorithm itself, and (3) it better handles broken surfaces.

For simplicity sake, the remainder of this section will often deal with the two-dimensional case, though we will still use the terms “plane” and “surface” instead of “curve” and “line” since all these concepts will apply to the 3D case as well.

Given a set of points (as shown in fig. 5), we compute the lower convex surface as shown.

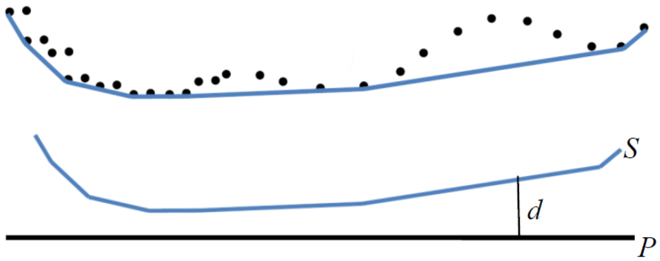


Fig. 5. Above: The lower convex envelope computed from a set of points. Below: A candidate datum plane *P* is shown along with its distance to a point of the surface.

It is important to emphasize that we now seek find the plane that minimizes the constrained L_2 objective function between the plane and convex surface, not the original points. So then, applying the constrained L_2 norm to the convex surface, we seek to minimize, from Eq. (1),

$$\int_S d^2(\boldsymbol{x}, P)\,ds\,, \tag{2}$$

where the plane *P* is constrained to lie on the non-material side of the convex surface *S*. It is immediately clear that the *P* that minimizes the objective function will contact *S*, since, if it did not, the objective function could be lowered by shifting *P* closer to *S*.

If *S* is obtained as the convex surface formed from discrete input points, then it is a piecewise linear surface. (In 3D it is a union of discrete triangles). For any candidate plane, *P*, the solution to equation (2) can be found by summing individual integrals along each line segment of *S*. But the solution to (2) over each line segment will be a 3rd degree polynomial.

However, the problem can be converted into a least-squares problem, which will allow a much more efficient numerical solution. Simpson’s rule [11] is a numerical integration technique that uses three function values at the left, right, and middle of an interval to approximate the integral of a function over an interval (fig. 6) and a similar method for integrating over a triangle in our 3D case. While Simpson’s rule is generally an approximation, it has been proved that it is exact for integrals of functions that are polynomials of degree 2, which is the case here. Therefore, we can solve (2) exactly over each line segment (or triangle) that comprises *S* in order to solve a minimum sum-of-squares problem using well known methods.

[3] We do not go into detail here about the disadvantages of a least-squares or shifted least-squares datum definition. That has been done in [10]. We only note here the advantage of its stability in order to show that the constrained L_2 definition contains a similar appealing property.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

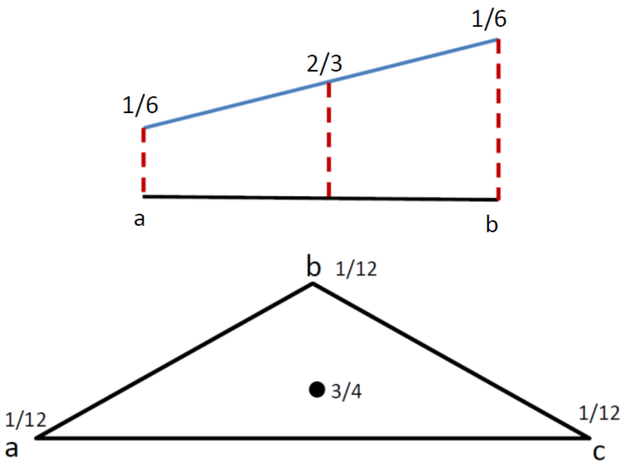


Fig. 6. The locations and weights for function evaluations for numerical integration using Simpson's rule over an interval and triangle.

Simpson's rule for integrating over an interval or triangle depends only on the weighted values of the function at the endpoints (vertices) and centroid. Over an interval, Simpson's rule is given by:

$$\int_a^b f(x)dx \approx (b-a)\left(\frac{1}{6}f(a) + \frac{2}{3}f\left(\frac{a+b}{2}\right) + \frac{1}{6}f(b)\right),$$

and for integrating over a triangle, T, as shown in fig. 6,

$$\int_T f(\boldsymbol{s})dT \approx$$

$$\text{Area}(T)\left(\frac{1}{12}f(a) + \frac{1}{12}f(b) + \frac{1}{12}f(c) + \frac{3}{4}f\left(\frac{a+b+c}{3}\right)\right).$$

If each line segment of S is called S_i having left endpoint $\boldsymbol{x_i}$, right endpoint $\boldsymbol{x_{i+1}}$, midpoint, $\boldsymbol{m_i}$, and length L_i, (i = 1, 2, …, N, the number of edges and where L denotes the total length, $L = \sum_{i=1}^{N} L_i$) then Simpson's rule gives the integral evaluation as

$$\int_{S_i} |d^2(\boldsymbol{x}, P)| ds = \tfrac{L_i}{6}[d^2(\boldsymbol{x_i}) + 4d^2(\boldsymbol{m_i}) + d^2(\boldsymbol{x_{i+1}})]. \quad (3)$$

Because Simpson's rule is exact for functions of degree 2, we note that in Eq (3) this is an exact calculation of the integral and not a mere approximation. (Simpson's rule is also exact for our 3D case). The framing of this problem as a weighted sum-of-squares now allows us to solve the objective function as a singular value decomposition problem. See [12] for a general treatment of the singular value decomposition as a method for minimizing the total least-squares problem, and [13] for an application of it applied to planar fitting with weighted points, which is our case here.

In the Appendix, we prove theorems 1 and 2, which when applied to our applications give us the remarkable result, that (in 2D) the objective function for any candidate plane P is given by the efficient formula:

$$\sigma_1^2 \text{Cos}^2\theta + \sigma_2^2 \text{Sin}^2\theta + Ld_c^2, \qquad (4b)$$

or equivalently

$$\sigma_1^2 a^2 + \sigma_2^2 b^2 + Ld_c^2, \qquad (4a)$$

where (see fig. 7) d_c is the distance from the plane P to the centroid, σ_1 and σ_2 are the singular values from the singular value decomposition (SVD, of the matrix $\boldsymbol{M}$ below), and θ represents the angle P makes with the singular vector corresponding to the smallest singular value, σ_1. (Eq. (4b) is just a restatement of (4a), where $(a, b) = (\text{Cos}\theta, \text{Sin}\theta)$ is the unit normal to the candidate plane expressed as dot products with the singular vectors.) The $3N \times 2$ matrix, $\boldsymbol{M}$, that is used in the singular value decomposition comes from the elements of Eq. (3), repeated for each of the N line segments:

$$\boldsymbol{M} = \sqrt{\frac{1}{6}}\begin{bmatrix} \sqrt{L_1}(x_1) & \sqrt{L_1}(y_1) \\ 2\sqrt{L_1}\left(\frac{x_1+x_2}{2}\right) & 2\sqrt{L_1}\left(\frac{y_1+y_2}{2}\right) \\ \sqrt{L_1}(x_2) & \sqrt{L_1}(y_2) \\ \vdots & \vdots \\ \sqrt{L_N}(x_N) & \sqrt{L_N}(y_N) \\ 2\sqrt{L_N}\left(\frac{x_N+x_{N+1}}{2}\right) & 2\sqrt{L_N}\left(\frac{y_N+y_{N+1}}{2}\right) \\ \sqrt{L_N}(x_{N+1}) & \sqrt{L_N}(x_{N+1}) \end{bmatrix}$$

(The construction of $\boldsymbol{M}$ is done with the data translated so the centroid is at the origin. This translation is not shown explicitly in the matrix due to lack of space. See Theorem 1 in the appendix for further details.)

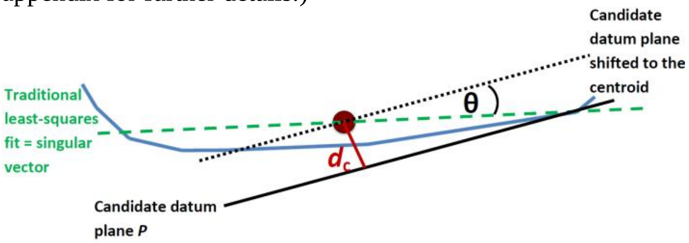

Candidate datum plane shifted to the centroid
Traditional least-squares fit = singular vector
θ
d_c
Candidate datum plane P

Fig. 7. The objective function for any candidate datum can be found simply by finding the angle θ and distance d_c and using Eq. (4).

Using Eq. (4) to compute the objective function means that the singular value decomposition only has to be computed once and its result can be applied to any given candidate datum plane. This makes for a much more efficient minimization algorithm.

What is fascinating about Eq. (4) is that the first two terms are exactly the objective function used in a traditional least-squares minimization while the last term is the objective function in an L_1 fit. And we will see that the objective function indeed does manifest itself as having the properties of both, which is what is desired.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

This can extend to 3D as well, since we showed that there is an extension of Simpson's rule that applies to integration over a triangular region. For the 3D case, the objective function for any candidate plane P is given by the efficient formula:

$$\sigma_1^2 a^2 + \sigma_2^2 b^2 + \sigma_3^2 c^2 + A d_c^2, \qquad (5)$$

where d_c is the distance from the plane P to the centroid, σ_1, σ_2 and σ_3 are the singular values from the singular value decomposition (SVD, of the matrix $\boldsymbol{M}$ below), and (a, b, c) is the unit normal to the candidate plane P expressed as the dot product of that normal with each of the three singular vectors. Applying Simpson's rule for each of the N triangles, the $4N \times 3$ matrix, $\boldsymbol{M}$, that is used in the singular value decomposition is:

$$\boldsymbol{M} = \sqrt{\frac{1}{12}} \begin{bmatrix} \sqrt{A_1}x_{1\mathrm{A}} & \sqrt{A_1}y_{1\mathrm{A}} & \sqrt{A_1}z_{1\mathrm{A}} \\ \sqrt{A_1}x_{1\mathrm{B}} & \sqrt{A_1}y_{1\mathrm{B}} & \sqrt{A_1}z_{1\mathrm{B}} \\ \sqrt{A_1}x_{1\mathrm{C}} & \sqrt{A_1}y_{1\mathrm{C}} & \sqrt{A_1}z_{1\mathrm{C}} \\ 3\sqrt{A_1}\bar{x}_1 & 3\sqrt{A_1}\bar{y}_1 & 3\sqrt{A_1}\bar{z}_1 \\ \vdots & \vdots & \vdots \\ \sqrt{A_N}x_{N\mathrm{A}} & \sqrt{A_N}y_{N\mathrm{A}} & \sqrt{A_N}z_{N\mathrm{A}} \\ \sqrt{A_N}x_{N\mathrm{B}} & \sqrt{A_N}y_{N\mathrm{B}} & \sqrt{A_N}z_{N\mathrm{B}} \\ \sqrt{A_N}x_{N\mathrm{C}} & \sqrt{A_N}y_{N\mathrm{C}} & \sqrt{A_N}z_{N\mathrm{C}} \\ 3\sqrt{A_N}\bar{x}_N & 3\sqrt{A_N}\bar{y}_N & 3\sqrt{A_N}\bar{z}_N \end{bmatrix}$$

(The construction of $\boldsymbol{M}$ is done with the data translated so the centroid is at the origin. This translation is not shown explicitly in the matrix due to lack of space. See Theorem 1 in the appendix for further details.)

The notation used in showing $\boldsymbol{M}$ (just above) assumes the surface is comprised of N triangles T_i , each having area A_i and vertices ($x_{i\mathrm{A}}$, $y_{i\mathrm{A}}$, $z_{i\mathrm{A}}$), ($x_{i\mathrm{B}}$, $y_{i\mathrm{B}}$, $z_{i\mathrm{B}}$), and ($x_{i\mathrm{C}}$, $y_{i\mathrm{C}}$, $z_{i\mathrm{C}}$), their average being $(\bar{x}_i, \bar{y}_i, \bar{z}_i)$

We can summarize the 3D constrained L_2 algorithm as follows (the 2D case being similar):

Given:

1) Data points $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \cdots, \boldsymbol{x}_M$, where each $\boldsymbol{x}_i = (x_i, y_i, z_i,)$, and
2) A direction, $\boldsymbol{a}^*$ that indicates the direction into the material,

then the datum plane is established using the following steps:

1) Compute the convex hull of the data points and represent it by the union of a set of triangles.
2) Select the N triangles (where $N < M$) that are exterior to the material (i.e., the triangles that comprise the lower convex envelope). This can be accomplished by computing the normal to each triangle (pointing into the hull) and comparing its direction to $\boldsymbol{a}^*$. (The sign of the dot product can easily be used here).
3) Compute the centroid, $\bar{\boldsymbol{x}}$, of the convex surface of Step 2. The centroid of each triangle can be trivially computed as the average of its vertices. The sum of these centroids when weighted by their relative areas is the centroid of the lower convex envelope. If the N triangles each has area A_i, then each relative weight is $w_i = A_i / \sum_{i=1}^{N} A_i$.
4) Construct the matrix $\boldsymbol{M}$ as defined above and compute its singular value decomposition to obtain the singular values σ_1 , σ_2 and σ_3 and their corresponding singular vectors.
5) The objective function can now be used efficiently in a minimization algorithm to find the optimal plane that is constrained to lie on one side of the material. Given any candidate orientation, the candidate plane can be found easily by shifting it just to the outer edge of the material. The objective function of this candidate plane can be easily computed using Eq. (5).

Before moving on to the next section that highlights why the algorithm is so appealing to the standards writers, we note that the only three nontrivial mathematical functions needed for implementation of this algorithm are (1) a convex hull function, (2) a singular value decomposition function, and (3) a minimization function. All three of these are well researched, documented, and available to the numerical community. In fact, the minimization algorithm (3) can be eliminated, as is explained in the code in the appendix, where an even more efficient solution is explained.

5. THE APPEALING PROPERTIES OF THE CONSTRAINED L_2 DATUM PLANE DEFINITION

When we saw that the L_2 constrained objective function in Eq. (4) was in fact a combination of L_1 and traditional least-squares objective functions, we suspected that this datum plane definition might manifest itself as combining the advantageous properties of them both. This turns out to be the case. Figure 8 shows two typical cases where, on the left, one would seek to balance the rocking condition, and on the right, one would seek for the datum plane to be stably flush with the edge of the datum feature. This is what the constrained L_2 solution does automatically.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

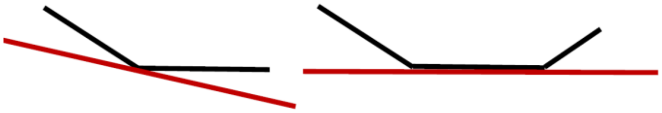


Fig. 8. Two typical cases of datum features with the associated constrained L_2 datums shown. The balanced rocking case is on the left and the stable, flush case is on the right.

For the rocker condition pictured on the left side of fig. 8, if the line segment on the right were made longer, the constrained L_2 datum plane would roll to the right smoothly. For the stable case pictured on the right side of fig. 8, if the line segment on the right were made somewhat longer, the L_2 constrained datum plane would not move from its stable state. It would remain flush with the edge of the datum feature until the line segment on the right grew long enough to make a rocker condition, at which point the L_2 constrained datum would smoothly begin to roll to the right to balance the rocker.

In contrast, the shifted least-squares solution would achieve a flush mating with the datum feature (as pictured on the right of fig. 8) for only an instant. That is, as the line segment on the right began to be extended, there would only be one length that resulted in a flush mating. This contrast shows the fascinating feature of the constrained L_2, which stays flush with the datum feature—even while the line segment extends—until it reaches such a length that a rocking condition exists, like shown in fig. 9.

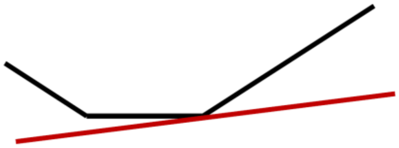


Fig. 9. The line segment on the right is long enough for the constrained L_2 datum to treat it as a rocking condition and separate from the flush contact it had in the right hand picture of fig. 8.

6. CONCLUSIONS

The constrained L_2 datum definition for planes has the remarkable benefit of combining desired properties from both the constrained L_1 definition and traditional least-squares definition, which each have their deficiencies by themselves. We have shown that the objective function in the constrained L_2 definition actually can be mathematically broken down to be seen (perhaps unexpectedly) as a combination of the objective functions of the constrained L_1 and traditional least-squares. Furthermore, a careful application of Simpson's rule and singular value decomposition (which is widely available) allows for the objective function to be evaluated efficiently and solved with popular optimization algorithms. 2D code in Matlab is provided in the appendix for the reader and has been evaluated in numerous test cases to be found appealing in its behavior and stable in its results.

REFERENCES

[1] Srinivasan, V., "Reflections on the role of science in the evolution of dimensioning and tolerancing standards," Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, Vol. 227, No. 1, pp. 3-11, 2013. DOI: 10.1177/0954405412464012

[2] Tandler, W. "All Those Datum Things" *Inside Metrology*, Quality Digest, Quality Digest Magazine, 13 February 2008.

[3] Tandler, W. "Establishing Datum Reference Frames," *Inside Metrology*, Quality Digest, 12 March 2008.

[4] ANSI/ASME Y14.5.1M-2009 "Dimensioning and Tolerancing," The American Society of Mechanical Engineers, New York.

[5] ANSI/ASME Y14.5.1M-1994 "Dimensioning and Tolerancing," The American Society of Mechanical Engineers, New York.

[6] ISO 5459:2011. "Geometrical product specifications (GPS)—geometrical tolerancing—datums and datum systems." Geneva: International Organization for Standardization, 2011.

[7] Zhang, Xuzeng, and Roy, Utpal "Criteria for establishing datums in manufactured parts" Journal of Manufacturing Systems, 12(1), pp 36–50, 1993.

[8] Shakarji, C. M., and Srinivasan V., "Theory and Algorithms for L1 Fitting Used for Planar Datum Establishment in Support of Tolerancing Standards," DETC2013-12372, Proceedings, ASME 2013 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Portland, OR, 2013.

[9] Hopp, T. H., 1990, "The Mathematics of Datums," ASPE Newsletter, September 1990, American Society for Precision Engineering, Raleigh, NC. A reprint is available at: http://www.mel.nist.gov/msidlibrary/doc/hopp90.pdf

[10] Shakarji, C. M., and Srinivasan V., "An improved L1 based algorithm for stnadardized planar datum establishment," DETC2014-35461, Proceedings, ASME 2014 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Buffalo, NY, 2014.

[11] Horowitz, A., "A version of Simpson's rule for multiple integrals," Journal of Computational and Applied Mathematics 134 (2001) 1–11.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

[12] VanHuffel, S., and Vandervalle, J., 1991 The Total Least Squares Problem: Computational Aspects and Analysis, SIAM, Philadelphia, PA.

[13] Shakarji, C. M., and Srinivasan, V., “Theory and Algorithms for Weighted Total Least-Squares Fitting of Lines, Planes, and Parallel Planes to Support Tolerancing Standards,” ASME Journal of Computing and Information Science in Engineering, 13(3), 2013.

[14] "Singular Value Decomposition" Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc. 10 Aug. 2015. https://en.wikipedia.org/wiki/Singular_value_decomposition

APPENDIX: PROOF OF THE EFFICIENT OBJECTIVE FUNCTION FORMULAS

Two theorems need to be proved in order to justify Eqs (4) and (5). They are closely related to the well-known principal axis theorem and parallel axis theorem. The 3D and 2D proofs are similar, and one can infer one straightforwardly from the other, so to minimize cumbersome notation, we show the 3D case.

Theorem 1. *Assume that we are given a set of data points* $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_N\}$, *where* $\boldsymbol{x}_i = (x_i, y_i, z_i)$, *and the corresponding positive weights:* $w_1, w_2, \cdots w_N$, *where all the weights are positive and where the centroid (i.e. the weighted centroid,* $\frac{\sum_{i=1}^N w_i x_i}{\sum_{i=1}^N w_i}$) *is expressed as* $\bar{\boldsymbol{x}} = (\bar{x}, \bar{y}, \bar{z})$. *Then the sum of the squares of the distances from these points to a plane passing through the centroid is* $\sigma_1^2 a^2 + \sigma_2^2 b^2 + \sigma_3^2 c^2$, *where* σ_1, σ_2 *and* σ_3 *are the singular values of* $\boldsymbol{M}$ *(as defined below) and* (a, b, c) *is the unit normal to the plane expressed in terms of the eigenvectors of* $\boldsymbol{M}$.

Proof: For a plane passing through the centroid, having unit normal $\boldsymbol{n} = (n_1, n_3, n_3)$, define the sum-of-squares of the distances as

$$F(\boldsymbol{n}) = \sum_{i=1}^{N} w_i d_i^2 = \sum_{i=1}^{N} w_i [\boldsymbol{n} \cdot (\boldsymbol{x}_i - \bar{\boldsymbol{x}})]^2.$$

Let $G(\boldsymbol{n}) = 0$ be the constraint that $\boldsymbol{n}$ be a unit vector (where $G(\boldsymbol{n}) = |\boldsymbol{n}|^2 - 1$). Using the method of Lagrange multipliers, we know that the critical points of $F(\boldsymbol{n})$ subject to the constraint that $G(\boldsymbol{a}) = 0$ occurs when $\nabla F = \lambda \nabla G$. In this case we have,

$$\nabla F = \begin{bmatrix} \dfrac{\partial F}{\partial n_1} \\ \dfrac{\partial F}{\partial n_2} \\ \dfrac{\partial F}{\partial n_3} \end{bmatrix},$$

which, when expanded becomes:

$$2\begin{bmatrix} \sum_{i=1}^{N} w_i [\boldsymbol{n} \cdot (\boldsymbol{x}_i - \bar{\boldsymbol{x}})](x_i - \bar{x}) \\ \sum_{i=1}^{N} w_i [\boldsymbol{n} \cdot (\boldsymbol{x}_i - \bar{\boldsymbol{x}})](y_i - \bar{y}) \\ \sum_{i=1}^{N} w_i [\boldsymbol{n} \cdot (\boldsymbol{x}_i - \bar{\boldsymbol{x}})](z_i - \bar{z}) \end{bmatrix},$$

which can be rewritten as

$$2\begin{bmatrix} w_i(x_i - \bar{x})^2 & w_i(x_i - \bar{x})(y_i - \bar{y}) & w_i(x_i - \bar{x})(z_i - \bar{z}) \\ w_i(x_i - \bar{x})(y_i - \bar{y}) & w_i(y_i - \bar{y})^2 & w_i(y_i - \bar{y})(z_i - \bar{z}) \\ w_i(x_i - \bar{x})(z_i - \bar{z}) & w_i(y_i - \bar{y})(z_i - \bar{z}) & w_i(z_i - \bar{z})^2 \end{bmatrix} \begin{bmatrix} n_1 \\ n_2 \\ n_3 \end{bmatrix},$$

where each entry in the 3 × 3 matrix is understood as being summed from 1 to *N*. However, the 3 × 3 shown can be written as $\boldsymbol{M}^T\boldsymbol{M}$ where $\boldsymbol{M}$ is defined as the $N \times 3$ matrix

$$\boldsymbol{M} = \begin{bmatrix} \sqrt{w_1}(x_1 - \bar{x}) & \sqrt{w_1}(y_1 - \bar{y}) & \sqrt{w_1}(z_1 - \bar{z}) \\ \sqrt{w_2}(x_2 - \bar{x}) & \sqrt{w_2}(y_2 - \bar{y}) & \sqrt{w_2}(z_2 - \bar{z}) \\ \vdots & \vdots & \vdots \\ \sqrt{w_N}(x_N - \bar{x}) & \sqrt{w_N}(y_N - \bar{y}) & \sqrt{w_N}(z_N - \bar{z}) \end{bmatrix}.$$

We also have $\nabla G = 2\boldsymbol{n}$ making $\nabla F = \lambda \nabla G$ become a 3 × 3 eigen-problem given by

$$\boldsymbol{M}^T\boldsymbol{M} \begin{bmatrix} n_1 \\ n_2 \\ n_3 \end{bmatrix} = \lambda \begin{bmatrix} n_1 \\ n_2 \\ n_3 \end{bmatrix}.$$

These three equations can be written:

$$\sum_{i=1}^{N} w_i (x_i - \bar{x})[\boldsymbol{n} \cdot (\boldsymbol{x}_i - \bar{\boldsymbol{x}})] = \lambda n_1$$
$$\sum_{i=1}^{N} w_i (y_i - \bar{y})[\boldsymbol{n} \cdot (\boldsymbol{y}_i - \bar{\boldsymbol{y}})] = \lambda n_2$$
$$\sum_{i=1}^{N} w_i (z_i - \bar{z})[\boldsymbol{n} \cdot (\boldsymbol{z}_i - \bar{\boldsymbol{z}})] = \lambda n_3$$

Multiplying these equations by n_1, n_2, and n_3 respectively, then summing the equations gives

$$\textstyle\sum_{i=1}^{N} w_i [\boldsymbol{n} \cdot (\boldsymbol{x}_i - \bar{\boldsymbol{x}}_{\boldsymbol{A}})]^2 = \lambda |\boldsymbol{n}|^2 = \lambda \qquad (6)$$

But the sum on the left is just the objective function, $F(\boldsymbol{a})$, hence the sum of squares of the distances to a plane passing through the centroid (when the plane’s normal is an eigenvector of $\boldsymbol{M}^T\boldsymbol{M}$) is equal to the eigenvalue (λ) corresponding to that eigenvector. We note $\boldsymbol{M}^T\boldsymbol{M}$ is a real, symmetric matrix and thus its eigenvectors are orthogonal (and can be assumed to orthonormal by simple scaling).

Now consider the more general case of any plane *P* passing through the centroid (not necessarily having its normal as one of the eigenvectors) whose unit normal is $\boldsymbol{a} = (a, b, c)$ when expressed in terms of the orthonormal eigenvectors of $\boldsymbol{M}^T\boldsymbol{M}$.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

(The eigenvectors are being used as a basis to express the normal to the plane.) The Pythagorean Theorem can be used to show the square of the orthogonal distance from each point to the plane is equal to the sum of the squares of the distances from the point to the three orthogonal planes formed by the eigenvectors. (Figure 10 shows a 2D depiction).

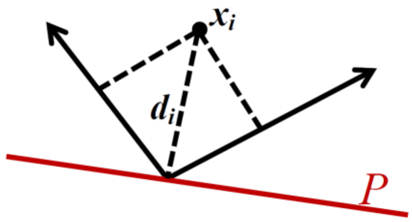


Fig. 10. The distance from a point to a plane is decomposed into separate distances to the orthogonal planes formed as normal to the eigenvectors.

Therefore, the sum of the squares of the distances from the points to P can be grouped by distances to each orthogonal plane and then the sum of the squares for each group can be replaced by the eigenvalue associated with its plane as we showed. Thus if the eigenvalues are labeled λ_1, λ_2, and λ_3, then the sum of the squares of the orthogonal distances to the plane P is simply

$$a^2\lambda_1 + b^2\lambda_2 + c^2\lambda_{3.}$$

Because the singular vectors from the singular value decomposition of $\boldsymbol{M}$ are the same as the eigenvectors of $\boldsymbol{M}^T\boldsymbol{M}$ [14], and since the singular values of $\boldsymbol{M}$ are the square root of the singular values of $\boldsymbol{M}^T\boldsymbol{M}$ [14], we have that the sum of the squares of the distances can be restated as

$$a^2\sigma_1^2 + b^2\sigma_2^2 + c^2\sigma_3^2. \qquad ■$$

Theorem 1 is related to the principal axis theorem. The following theorem, related to the parallel axis theorem, states that when a plane is translated away from passing through the centroid, the increase to the sum-of-squares of the distances increases by an easily computed amount, namely the square of the distance moved times the sum of the weights. In our application, the sum of the weights is the total area (in 3D) or the total length (in 2D).

Theorem 2. *Assume that we are given a set of data points* $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_N\}$, *where* $\boldsymbol{x}_i = (x_i, y_i, z_i)$, *and the corresponding positive* weights*:* $w_1, w_2, \cdots w_N$, *where all the weights are positive and where the centroid (i.e. the weighted centroid,* $\frac{\sum_{i=1}^N w_i x_i}{\sum_{i=1}^N w_i}$*) is expressed as* $\overline{\boldsymbol{x}} = (\bar{x}, \bar{y}, \bar{z})$. *Assume also that* α *represents the sum of squares of the distances from that plane to a plane P passing through the centroid. If P* is parallel to P but separated from by a distance* d_c*, then the sum of squares of the distances from the points to P* is* $\alpha + d_c^2 \sum_{i=1}^N w_i$.

Proof: Given that $\alpha = \sum_{i=1}^N w_i d_i^2$, we seek to find $\sum_{i=1}^N w_i (d_i + d_c)^2$. Expanding the square yields

$$\sum\nolimits_{i=1}^{N} w_i d_i^2 + d_c^2 \sum\nolimits_{i=1}^{N} w_i + 2d_c \sum\nolimits_{i=1}^{N} w_i d_i.$$

But the first term is just α and the last term is zero. The last term must be zero, since

$$\sum\nolimits_{i=1}^{N} w_i d_i = \sum\nolimits_{i=1}^{N} w_i [\boldsymbol{n} \cdot (\boldsymbol{x}_i - \overline{\boldsymbol{x}})] =$$

$$\boldsymbol{n} \cdot \left[\sum\nolimits_{i=1}^{N} w_i \, \boldsymbol{x}_i - \overline{\boldsymbol{x}} \sum\nolimits_{i=1}^{N} w_i\right],$$

And substituting $\frac{\sum_{i=1}^N w_i x_i}{\sum_{i=1}^N w_i}$ for $\overline{\boldsymbol{x}}$ causes the bracketed term to vanish. Thus the shift by d_c caused the sum of squares to become

$$\alpha + d_c^2 \sum\nolimits_{i=1}^{N} w_i \qquad ■$$

In our application of this theorem, the weights are the areas of the triangles (or the the lengths of the line segments in 2D) so the sum of the weights is the total area A (or total length L in 2D). The shift of a plane by an amount d_c as shown in fig. 7 results in an addition to the sum-of-squares of Ad_c^2 in 3D or Ld_c^2 in 2D.

APPENDIX: 2D CODE IN MATLAB

The algorithm documented in this paper showed how the objective function could be efficiently expressed and used in a minimization algorithm. However, the (2D) code below employs an even faster method. Specifically, Eq. (4) is used to find the line coincident with a line segment of the convex surface that minimizes the objective function. Then both endpoints of that line segment are evaluated to see if balancing a rocker condition on either vertex improves the objective function. These tests on the two endpoints are achieved using two other calculations of the singular value decomposition. While the details of this are not gone into in this paper, it has been tested in over 250,000 test cases with simulated data sets to ensure the exact equivalence. Thus the faster algorithm is given here.

Though 3D code is not included here, Eq. (5) can be used to find the triangle that minimizes the objective functions. Then similar tests could be used to check the vertices and edges of that triangle to see if balancing a rocker condition (on an edge or point) improves the sum-of-squares.

```
function [point, direction] = L2C2Dline(originalpts,
refdir)
% L2C2Dline returns the line that minimizes the sum-
% of-squares of distances between the line and the
% lower convex envelope of a set of points ("lower"
% as determined by refdir) and such that the line is
% constrained to lie on the lower side of the convex
% envelope. The function can be used, for example, as
% [point, direction] = L2C2Dline(originalpts, refdir)
```

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

```
%
%  The function returns [point, direction] where
% "point" is a point on the line and "direction" is a
% unit vector giving the direction of the line.
% "orignalpts" is an N X 2 matrix of points: [x1
% y1;x2 y2;...;xN yN] and "refdir" is a direction [x
% y] (not = {0, 0}) that points into the material.
% "refdir" allows the algorithm to know on which side
% of the points the line must lie. Generally, refdir
% does not need to be known very accurately. The
% number of points, N, must be at least two.
%
% Check for the two point case:
%
if (size(originalpts,1) == 2)
    point = sum(originalpts)/size(originalpts,1);
    direction = originalpts(2,:)-originalpts(1,:);
    direction = direction/norm(direction);
    if ([refdir(2) -refdir(1)]*[direction]' < 0)
        direction = -direction;
    end
    else

%
% Translate and rotate the original data set, so that
% the points are close to the origin and so that
% refdir points in the direction of the +y-axis.
%
translation = sum(originalpts)/size(originalpts,1);
pts = bsxfun(@minus,originalpts,translation);
dir = refdir/norm(refdir);
pts = pts*[dir(2) dir(1);-dir(1) dir(2)];
%
% Now that the point lie somewhat along the x-axis,
% sort them according to increasing x-values
%
[~,indices]=sort(pts(:,1));
pts = pts(indices,:);

indices = convhull(pts(:,1),pts(:,2));
pts = pts(indices,:);

midpts = (pts(2:end,:) + pts(1:end-1,:))/2;
vectors = pts(2:end,:) - pts(1:end-1,:);
pts = pts(1:end-1,:);
normals = [-vectors(:,2) vectors(:,1)];
indices = normals(:,2) > 0;
pts = pts(indices,:);
midpts = midpts(indices,:);
vectors = vectors(indices,:);
normals = normals(indices,:);
pts = [pts;pts(end,:)+vectors(end,:)];
%
% Now "pts" contains only the vertices of the lower
% convex envelope. We now compute a single Singular
% Value Decomposition that can be used to obtain the
% objective function values for all the lines
% containing edges of the lower convex envelope.
%
normals = bsxfun(@rdivide,normals,rssq(normals,2));
lengths = rssq(vectors,2);
L = sum(lengths);
centroid = lengths'*midpts/L;

weights = ([lengths;0] + [0;lengths])/6;
shiftedpts = bsxfun(@minus,pts,centroid);
weightedpts =
bsxfun(@times,shiftedpts,sqrt(weights));
shiftedmidpts = bsxfun(@minus,midpts,centroid);
weightedmidpts =
bsxfun(@times,shiftedmidpts,sqrt((2/3)*lengths));
allweightedpts = [weightedpts; weightedmidpts];

[~,S,V] = svd(allweightedpts,0);
ssq1 = S(2,2)^2;
ssq2 = S(1,1)^2;
direction = V(:,1)';
if direction(1) < 0
    direction = -direction;
end

angleSVD = atan2(direction(2),direction(1));
angles = atan2(vectors(:,2),vectors(:,1));
anglediffs = angles - angleSVD;
objfunangle = ssq1*(cos(anglediffs)).^2  +
ssq2*(sin(anglediffs)).^2;
ds = dot(normals',-shiftedmidpts')';
objfunedges = objfunangle + L*ds.^2;

[bestobjvalue,minedgeindex] = min(objfunedges);
bestdirection =
[cos(angles(minedgeindex)),sin(angles(minedgeindex))]
;
bestpoint = midpts(minedgeindex,:);
%
% Now that the best edge has been found, we look at
% the endpoints of that edge to see if a line
% (external to the material) passing through either
% endoint gives a better objective function. This
% will involve one Singular Value Decomposition for
% each of the two endpoints.
%
for ii = minedgeindex:minedgeindex+1
    pt = pts(ii,:);
    shiftedpts = bsxfun(@minus,pts,pt);
    weightedpts =
(bsxfun(@times,shiftedpts,sqrt(weights)));
    shiftedpts = bsxfun(@minus,midpts,pt);
    weightedmidpts =
bsxfun(@times,shiftedpts,sqrt((2/3)*lengths));
    allweightedpts = [weightedpts; weightedmidpts];

    [~,S,V] = svd(allweightedpts,0);
    direction = V(:,1)';
    if direction(1) < 0
        direction = -direction;
    end

    normal = [-direction(2) direction(1)];
    shiftedpts=(bsxfun(@minus,pts,pt));
    dists = (normal*shiftedpts')';
    [~,minindex]=min(dists);

    if (minindex == ii && S(2,2)^2 < bestobjvalue)
        bestobjvalue = S(2,2)^2;
        bestdirection = direction;
        bestpoint = pt;
    end
end
point = translation + bestpoint*[dir(2) -
dir(1);dir(1) dir(2)];
direction = bestdirection*[dir(2) -dir(1);dir(1)
dir(2)];
end
end
```

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 00 (2016) 000–000

www.elsevier.com/locate/procedia

14th CIRP Conference on Computer Aided Tolerancing (CAT)

Theory and algorithm for planar datum establishment using constrained total least-squares

Craig M. Shakarji[a], Vijay Srinivasan[b]

[a]Physical Measurement Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899, craig.shakarji@nist.gov
[b]Engineering Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899, vijay.srinivasan@nist.gov

Abstract

First, we present an efficient algorithm for establishing planar datums that is based on a constrained minimization search based on the L2 norm after forming a convex surface from sampled points. Visualized by Gauss maps, we prove that the problem reduces to a minimization search where the global minimum is localized about the minimizing facet. Second, we highlight advantages of this planar datum, including the major advantage that the datum planes have full mechanical contact with the datum features in stable cases yet are automatically balanced for rocking conditions. These advantages make this definition appealing for standardization.

© 2016 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the organizing committee of the 14th CIRP Conference on Computer Aided Tolerancing.

Keywords: constrained least squares; constrained optimization; convex hull; datum; Gauss map; least squares; fitting; optimization; planar datum; singular value decomposition; total least squares

1. Introduction

In the world of Geometric Dimensioning and Tolerancing (GD&T), datums are used extensively to locate and orient tolerance zones [1-7]. Datum planes in particular are common and are established by mating planes to imperfect datum features on parts during inspection [3] (see Fig. 1). Distances and orientations on drawings and three-dimensional models are established from these datum planes, relative to which tolerance zones are located and oriented. Additional details of the importance and prevalence of datum planes in specifications are given in [8] and will not be revisited in this paper.

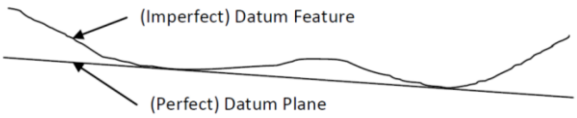


Fig. 1. Deriving a datum plane from a datum feature.

Given that datum planes are ubiquitous, it might be surprising that—short of standardization—there are several different yet reasonable approaches by which a datum plane can be established from a datum feature [9]. Furthermore, the International Organization for Standardization (ISO) and the American Society for Mechanical Engineering (ASME) are actively working to establish default datum plane definitions. In [10] we introduced a definition for a planar datum that naturally combines a correspondence to physical, surface plate mating (i.e., "high points") but with automatic balancing in the case of unstable, rocking conditions. The datum plane definition is based on a constrained total least-squares criterion (abbreviated here as L2C), which is explored in this paper. This should not be confused with an unconstrained total least-squares fit that is shifted out of the material.

Given a set of points sampled on a datum feature, the two major steps in establishing the L2C datum plane are as follows:

1) Compute the "lower" convex envelope of those points. This is the portion of the convex hull that lies on the nonmaterial side of the datum feature. In 3D, this convex envelope consists of a union of non-overlapping triangles, while in 2D it is a union of line segments creating a piecewise linear curve.
2) Find the plane, constrained to lie on the nonmaterial side of the computed convex surface that minimizes the integral of squared distances from that surface, namely $\int_S d^2(\boldsymbol{p}, P)ds$, where S is the convex surface and d is the distance from a point $\boldsymbol{p}$ on the surface to the

2212-8271 © 2016 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the organizing committee of the 14th CIRP Conference on Computer Aided Tolerancing.

plane, P. If P contains $\boldsymbol{x}$ and has normal $\boldsymbol{a}$, then $d = \boldsymbol{a} \cdot (\boldsymbol{p} - \boldsymbol{x})$.

Concentrating on the second step, we find the need to integrate over a set of triangles (or line segments in 2D). For each triangle (or line segment) this integral can be replaced by the Simpson's rule approximation (see Fig. 2) [11] (which we will see is actually exact in our case).

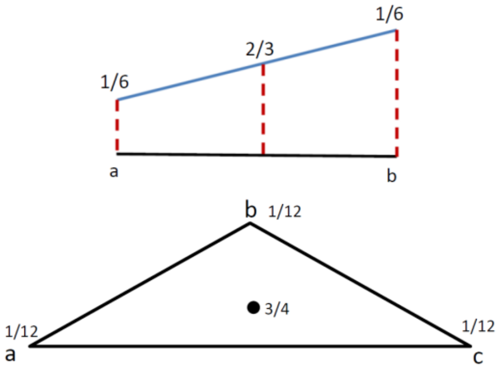


Fig. 2. The locations and weights for function evaluations for numerical integration using Simpson's rule over an interval and triangle.

Simpson's rule for integrating over an interval (or triangle for the 3D case) depends only on the weighted values of the function at the endpoints (or vertices in 3D) and at the centroid. Over an interval, Simpson's rule is given by:

$$\int_a^b f(x)dx \approx (b-a)\left(\frac{1}{6}f(a) + \frac{2}{3}f\left(\frac{a+b}{2}\right) + \frac{1}{6}f(b)\right),$$

and for integrating over a triangle, T, as shown in Fig. 2,

$$\int_T f(\boldsymbol{s})dT \approx$$

$$\text{Area}(T)\left(\frac{1}{12}f(a) + \frac{1}{12}f(b) + \frac{1}{12}f(c) + \frac{3}{4}f\left(\frac{a+b+c}{3}\right)\right).$$

Because Simpson's rule [11] is exact for functions of degree 2 (our case), we note that in the two formulas just above, these are exact calculations of the integrals and not mere approximations. The framing of this problem as a weighted sum-of-squares now allows us to solve the objective function as a singular value decomposition (SVD) problem. See [12] for a general treatment of using the SVD as a method for minimizing the total least-squares problem, and [13] for an application of it applied to planar fitting with weighted points (essential to be physically correct), which is our case here.

For the 3D case, let a S be a lower convex surface be made up of N triangles, T_1, T_2, …,T_N, where T_i has vertices (x_{iA}, y_{iA}, z_{iA}), (x_{iB}, y_{iB}, z_{iB}), and (x_{iC}, y_{iC}, z_{iC}) and where each triangle has centroid $(\bar{x}_i, \bar{y}_i, \bar{z}_i)$ and area A_i. If P is a candidate plane and, for each triangle, d_{iA}, d_{iB}, d_{iC} are the distances between P and the vertices and $\bar{d}_i$ is the distance from P to the triangle's centroid. Then, the L2C objective function to be minimized is:

$$\sum_{i=1}^{N} A_i\left(\frac{d_{iA}^2}{12} + \frac{d_{iB}^2}{12} + \frac{d_{iC}^2}{12} + \frac{3\bar{d}_i^2}{4}\right). \qquad (1)$$

For the 2D case, where the convex surface is comprised of $N-1$ line segments, each having length L_i , endpoints (x_i, y_i), and (x_{i+1}, y_{i+1}), d_i being the distance from P to (x_i, y_i), and $\bar{d}_i$ is the distance from P to the line segment's midpoint, we then have the objective function being

$$\sum_{i=1}^{N-1} L_i\left(\frac{d_i^2}{6} + \frac{d_{i+1}^2}{6} + \frac{2\bar{d}_i^2}{3}\right). \qquad (2)$$

In [10] we proved that the (2D) objective function for any candidate plane P is given by the elegant, efficient formula:

$$\sigma_1^2\text{Cos}^2\theta + \sigma_2^2\text{Sin}^2\theta + Ld_c^2, \qquad (3a)$$

or equivalently

$$\sigma_1^2 a^2 + \sigma_2^2 b^2 + Ld_c^2, \qquad (3b)$$

where (see Fig. 3) d_c is the distance from the plane P to the centroid, σ_1 and σ_2 are the singular values from the SVD of the matrix $\boldsymbol{M}$ below, and θ represents the angle P makes with the singular vector corresponding to the smallest singular value, σ_1 . Eqs. (3a) and (3b) are equivalent, where $(a,b) = (\text{Cos}\theta, \text{Sin}\theta)$ is the unit normal to the candidate plane when expressed as the dot product of that normal with each of the two singular vectors (e.g., a is the dot product of the unit normal to the plane with the first singular vector). The $3N \times 2$ matrix, $\boldsymbol{M}$, that is used in the SVD comes from the elements the Simpson's rule approximation (see [10] for more detail), repeated for each of the N line segments:

$$\boldsymbol{M} = \sqrt{\frac{1}{6}}\begin{bmatrix} \sqrt{L_1}(x_1) & \sqrt{L_1}(y_1) \\ 2\sqrt{L_1}\left(\frac{x_1+x_2}{2}\right) & 2\sqrt{L_1}\left(\frac{y_1+y_2}{2}\right) \\ \sqrt{L_1}(x_2) & \sqrt{L_1}(y_2) \\ \vdots & \vdots \\ \sqrt{L_N}(x_N) & \sqrt{L_N}(y_N) \\ 2\sqrt{L_N}\left(\frac{x_N+x_{N+1}}{2}\right) & 2\sqrt{L_N}\left(\frac{y_N+y_{N+1}}{2}\right) \\ \sqrt{L_N}(x_{N+1}) & \sqrt{L_N}(x_{N+1}) \end{bmatrix}$$

(The construction of $\boldsymbol{M}$ is done with the data translated so the centroid is at the origin. This translation is not shown explicitly in the matrix for reasons of space.)

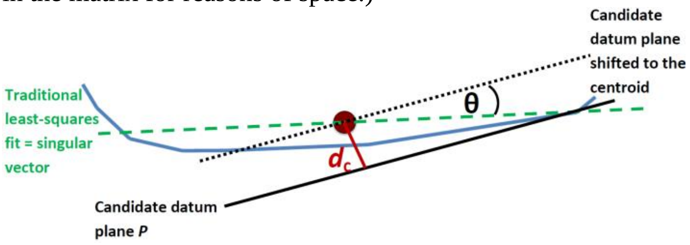

Candidate datum plane shifted to the centroid
Traditional least-squares fit = singular vector
θ
d_c
Candidate datum plane P

Fig. 3. The objective function for any candidate datum can be found simply by knowing the angle θ and distance d_c and using Eq. (3).

Using Eq. (3) to compute the objective function means that the SVD has to be computed only once, and its result can be applied to any given candidate datum plane. This makes for a much more efficient minimization algorithm.

What is fascinating about Eq. (3) is that the two terms on the left are exactly the objective function used in a traditional least-squares minimization while the term on the right is the objective function in a constrained L_1 fit [14, 15]. We will see that the objective function indeed does manifest itself as having the balancing property of the unconstrained least-squares and the full mechanical contact of the constrained L_1 definition, which is what is desired.

This can extend to 3D as well, since we showed that there is an extension of Simpson's rule that applies to integration over a triangular region. For the 3D case, the objective function for any candidate plane P is given by the efficient formula:

$$\sigma_1^2 a^2 + \sigma_2^2 b^2 + \sigma_3^2 c^2 + A d_c^2, \tag{4}$$

where d_c is the distance from the plane P to the centroid, σ_1, σ_2 and σ_3 are the singular values from the SVD of the matrix $\boldsymbol{M}$ below, and (a, b, c) is the unit normal to the candidate plane P when expressed as the dot product of that normal with each of the three singular vectors (e.g., a is the dot product of the unit normal to the plane with the first singular vector). Applying Simpson's rule for each of the N triangles, the $4N \times 3$ matrix $\boldsymbol{M}$ that is used in the SVD is:

$$\boldsymbol{M} = \sqrt{\frac{1}{12}} \begin{bmatrix} \sqrt{A_1}x_{1\mathrm{A}} & \sqrt{A_1}y_{1\mathrm{A}} & \sqrt{A_1}z_{1\mathrm{A}} \\ \sqrt{A_1}x_{1\mathrm{B}} & \sqrt{A_1}y_{1\mathrm{B}} & \sqrt{A_1}z_{1\mathrm{B}} \\ \sqrt{A_1}x_{1\mathrm{C}} & \sqrt{A_1}y_{1\mathrm{C}} & \sqrt{A_1}z_{1\mathrm{C}} \\ 3\sqrt{A_1}\bar{x}_1 & 3\sqrt{A_1}\bar{y}_1 & 3\sqrt{A_1}\bar{z}_1 \\ \vdots & \vdots & \vdots \\ \sqrt{A_N}x_{N\mathrm{A}} & \sqrt{A_N}y_{N\mathrm{A}} & \sqrt{A_N}z_{N\mathrm{A}} \\ \sqrt{A_N}x_{N\mathrm{B}} & \sqrt{A_N}y_{N\mathrm{B}} & \sqrt{A_N}z_{N\mathrm{B}} \\ \sqrt{A_N}x_{N\mathrm{C}} & \sqrt{A_N}y_{N\mathrm{C}} & \sqrt{A_N}z_{N\mathrm{C}} \\ 3\sqrt{A_N}\bar{x}_N & 3\sqrt{A_N}\bar{y}_N & 3\sqrt{A_N}\bar{z}_N \end{bmatrix}$$

(The construction of $\boldsymbol{M}$ is done with the data translated so the centroid is at the origin. This translation is not shown explicitly in the matrix for reasons of space.)

The notation used in showing $\boldsymbol{M}$ (just above) assumes the surface is comprised of N triangles T_i, each having area A_i and vertices $(x_{i\mathrm{A}}, y_{i\mathrm{A}}, z_{i\mathrm{A}})$, $(x_{i\mathrm{B}}, y_{i\mathrm{B}}, \mathrm{z}_{\mathrm{iB}})$, and $(x_{i\mathrm{C}}, y_{i\mathrm{C}}, z_{i\mathrm{C}})$, their average being $(\bar{x}_i, \bar{y}_i, \bar{z}_i)$.

We can summarize the 3D constrained L_2 algorithm as follows (the 2D case being similar): Given data points $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \cdots, \boldsymbol{x}_M$, where each $\boldsymbol{x}_i = (x_i, y_i, z_i,)$, and a direction that indicates the direction into the material, then the datum plane is established using the following steps:

1) Compute the convex hull of the data points and represent it by the union of a set of triangles.
2) Select the N triangles (where $N < M$) that are exterior to the material.
3) Compute the centroid, $\bar{\boldsymbol{x}}$, of the convex surface of Step 2.
4) Construct the matrix $\boldsymbol{M}$ as defined above and compute its SVD to obtain the singular values σ_1, σ_2, and σ_3 and their corresponding singular vectors.
5) The objective function can now be constructed by Eq (4) and used to find the optimal plane.

2. Gauss maps and convexity

The procedure to accomplish the optimization in Step 5 (just above) is not obvious. This section will use Gauss maps to describe the nature of the objective function, which will drive our choice of method to search for the optimal plane. In 2D, the search is for the optimal line with only one degree of freedom, namely the angle of the line (Fig. 4).

Thus we can envision a candidate datum line rolling (with increasing angle, as pictured in Fig. 4) from the left to the right, contacting different points and edges along the piecewise-linear curve. We note that the "rolling candidate line" will contact each vertex of the curve for some finite time, and coincide with each edge for only an instant before the point of contact shifts to the next vertex. This can be viewed as a Gauss map as in Fig. 5.

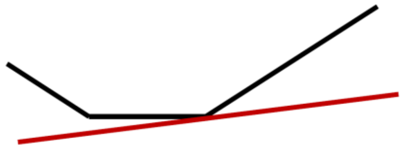


Fig. 4. A candidate datum is defined by its angle alone. Its location is automatically determined to just contact the curve.

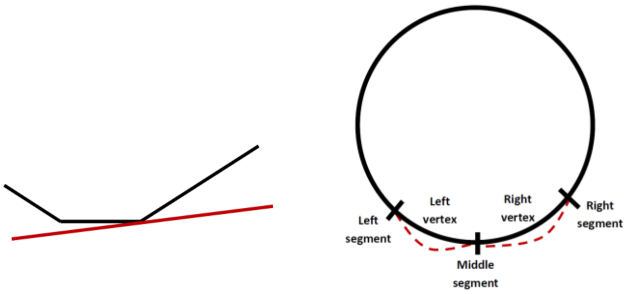


Fig. 5. (a) a rolling candidate line; (b) a 2D Gauss map showing a (dashed) example of a composite elliptical shape.

In this view, one can see that an edge on the curve corresponds to a point on the circle (Gauss map) and a vertex on the curve corresponds to an arc on the circle.

The objective function, when superimposed on the Gauss map, would be a composite elliptical shape. That is, the image of each arc on the circle would correspond to a part of an ellipse. (Note: the dashed curves in Fig. 5(b) show an example of a composite elliptical shape. It is not meant to correspond to the exact composite elliptical shape arising from the fig 5(a) to its left)

In 3D, there are two angular degrees of freedom in the optimization search. This can be visualized on a Gauss map using a sphere. The set of triangles that makeup the convex surface includes faces, edges, and vertices. The correspondences to the Gauss map are: triangular faces on the convex surface correspond to points on the sphere, edges on the convex surface correspond to edges on the sphere, and vertices on the convex surface correspond to (somewhat triangular) patches on the sphere. The objective function superimposed on the Gauss map forms a composite ellipsoidal shape, the 3D equivalent of the 2D case.

Realizing that the objective function has such a composite ellipsoidal/elliptical shape paves the way for the means to prove that the objective function is convex, a fact that is extremely helpful in creating an algorithm to efficiently find the global minimum.

3. The objective function is convex over the relevant search region.

We now give an outline of the proof that the objective function is convex with respect to any reasonable range of candidate orientations. Here, convexity is not a mere detail of technical interest but one we identify as a key accomplishment of this paper. Assurance of convexity is powerful, in that it allows for a much faster (and, in our case, non-iterative) solution to find the datum plane. Convexity of the objective function is not obvious, since the term Ld_c^2 that appears on the right of Eq (3) is not convex with respect to θ. Here we understand the objective function to be dependent solely on the candidate plane's orientation—its location is understood to be always just-contacting the convex surface.

We will first consider the 2D case, along with the assumption that the datum feature, and the discrete points arising from it, are approximately planar. (And thus the convex surface arising from the points is approximately planar.) This assumption is reasonable, since planar datums are nominally planes that typically have form deviations that are orders of magnitude smaller than their size. Even if the form deviation were, say, 10 % or 20 % of the extent of the planar patch (which would be an extremely large relative form error) the proof still holds, which is outlined in the following two steps.

Step 1: For each fixed vertex of the convex surface, the objective function (which is solely a function of the orientation, θ) is convex over each interval of θ that represents the rolling of the contacting plane about that vertex.

One way to see this is that we know the Gauss map of the objective function over the circular arc is an ellipse. This is shown in [16], which states that any linear transformation applied to the unit circle yields an image that is an ellipse. The size, shape, and orientation of the ellipse can be seen by the observing the SVD of the linear transformation matrix. Since the surface is nominally planar, the shape of the ellipse is predictably oriented and elongated similar to that as shown in Fig. 6. (Typically the elongation will be much more extreme than that shown.) Since the curvature of the ellipse between between θ_1 and θ_2 is sufficiently small, it is clear that a plot of the radial value of the ellipse between θ_1 and θ_2 is convex, as depicted in Fig. 6. The objective function is the square of the function shown in Fig. 7, but we note that the square of any nonnegative, convex function is also convex.

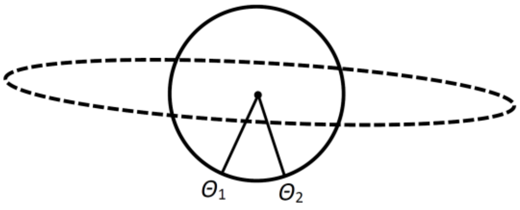


Fig. 6. A unit circle with its elliptical image.

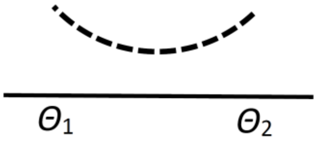


Fig. 7. The polar plot from θ_1 to θ_2 from Fig. 6 when expressed as a function of θ in a Cartesian graph.

We note that θ_1 and θ_2 would be limited, if needed, to conform to a reasonable range of candidate orientations.

Another way of demonstrating Step 1 is to observe that the objective function for a plane passing through a fixed vertex is

$$\sigma_1^2\text{Cos}^2\hat{\theta}+\sigma_2^2\text{Sin}^2\hat{\theta}, \qquad (5)$$

where σ_1 and σ_2 are the singular values from the SVD of the matrix $\widehat{\boldsymbol{M}}$ (which is $\boldsymbol{M}$ defined above, but with the data points shifted so that the vertex under consideration is the origin). $\hat{\theta}$ represents the angle P makes with the singular vector corresponding to the smallest singular value, σ_1, which is also the direction of the least-squares line constrained to pass through the vertex (Fig. 8). Since the second derivative of the function is a constant times $\text{Cos}(2\hat{\theta})$, and since a function is convex over the region that its second derivative is nonnegative, this function is convex for all angles, $\hat{\theta}$, between $-45°$ and $+45°$. This requirement is easily met under our assumption that the surface be somewhat planar.

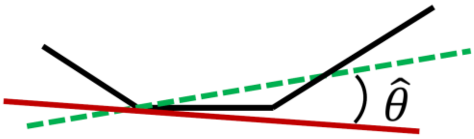


Fig. 8 The dashed line is the unconstrained least-squares fit to the piecewise linear curve, which is the basis from which the angle is measured for Eq. (5).

We note that it is indeed true that for the ends of the convex surface, a steep edge can exist, but we are only seeking to show the objective function is convex in the reasonable search range of values of θ, which excludes those extreme angles.

Step 2: The convexity from one piece of the graph to the next is preserved. Outline of proof of Step 2: The issue to be proven here is illustrated in Fig. 9. Depending on how the two functions come together determines whether convexity is preserved or broken.

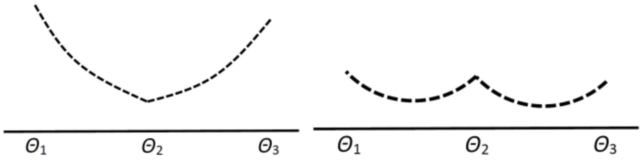


Fig. 9. (a) two convex functions over adjacent intervals result in a single convex function over the entire interval; (b) two convex functions over adjacent intervals result in a single nonconvex function over the interval.

Convexity can be proved by showing the first derivative is nondecreasing. Therefore we can prove that any two adjacent parts of the objective function come together in a manner like Fig. 9(a) rather than Fig 9(b) by comparing the derivative from the left with the derivative from the right. The derivative on the left equals the derivative on the right when observing the first two terms (on the left) in Eq (3a). However the third term (on the right) is different, since the vertex about which the candidate line rotates changes.

Three cases exist: In Case 1, as θ increases such that the candidate datum plane (line in 2D) rotates about vertex A, approaching the line segment, d_c (the distance to the centroid) is decreasing, see Fig. 10(a). Once θ increases past the line segment so that it is contacting and rotating about vertex B, d_c is increasing. Hence the derivative of the objective function is increasing through the transition from one piece to the next.

In Case 2, as θ increases such that the candidate datum plane (line in 2D) rotates about vertex A, approaching the line segment, d_c is decreasing, see Fig. 10(b). Once θ increases past the line segment so that it is contacting and rotating about vertex B, d_c is still decreasing but at a slower rate (seen by the lower "leverage" due to a closer fulcrum). Hence the derivative of the objective function is increasing through the transition from one piece to the next.

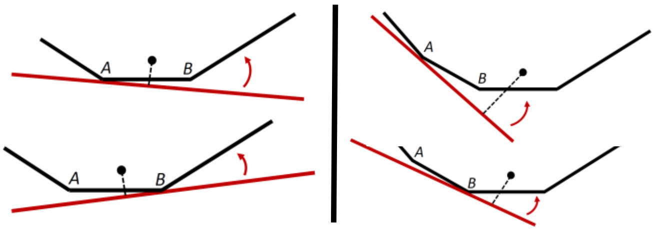


Fig. 10. As the point of contact shifts from A to B, (a) the distance to the centroid is decreasing then increasing, (b) the distance to the centroid is decreases more slowly (with respect to the angle).

Case 3 (not pictured, but somewhat like a mirror image of Fig. 11) is like case 2, but d_c is increasing in both cases, but increases at a faster rate after the transition from vertex A to vertex B.

While the 3D case is certainly more complicated and is not put in writing in this paper, there is nothing fundamentally different in extending Steps 1 and 2 to demonstrate convexity in that case as well with appropriate changes (e.g., 2D ellipses become 3D ellipsoids).

4. Convexity of the objective function leads to an efficient algorithm.

The fact that we can rely on the objective function to be convex has powerful implications for the efficiency of our fitting algorithm. In particular, we will show that convexity allows us to search for the minimizing facet and then simply test the boundaries of that minimizing facet for a global solution. Convexity assures that such a search captures the global minimum and does not miss some hidden minimum elsewhere.

Before giving an efficient, non-iterative algorithm, we note that the solution could be achieved by beginning with the orientation obtained using unconstrained total least-squares a starting orientation, and applying an iterative "downhill" minimization algorithm to the objective function as given in Eq. (1) (for 3D) or Eq. (2) (for 2D). For each candidate orientation, the candidate plane (or line in 2D) would be the one that just contacts the surface. Convexity assures that there is no risk of obtaining a local but not global minimum. While this may not be the most elegant approach, we mention it because it may be the simplest to code, which is desirable in some situations.

But convexity can also be used to create an efficient and elegant solution. One can perform an SVD to get the objective function in the form of Eq. (3) (for 2D) or Eq. (4) (for 3D) and use it to quickly compute the objective function for every triangular facet (or line segment in 2D).

In the 2D case, this step can be followed by checking the endpoints of the minimizing line segment to see if there exists a line passing through either endpoint that has a lower objective function and lies outside the material, see Fig. 11(a). This step can be achieved by—for each of the two endpoints—computing the SVD of the matrix matrix $\widehat{\boldsymbol{M}}$ (which is $\boldsymbol{M}$ defined above, but with the data points shifted so that the endpoint under consideration is the origin). Form the line passing through the endpoint and oriented in the direction of the singular vector corresponding to the smallest singular value. Convexity allows us to know that if that line lies outside the material, then it is the line that minimizes the objective function.

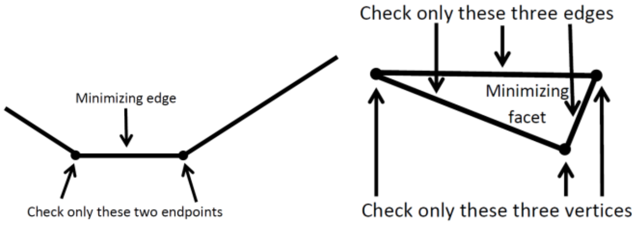

Minimizing edge
Check only these two endpoints
Check only these three edges
Minimizing facet
Check only these three vertices

Fig. 11. (a) the minimizing line will coincide with the minimizing edge or will balance on one of the two adjacent vertices;. (b) the minimizing plane will be coincident with the minimizing facet or balance on one of the adjacent edges or vertices. The triangle shown is one of a collection of triangles (not shown) that make up the convex surface, but only this triangle's edges and vertices need to be checked.

In 3D one can compute the centroid, shift to it, and then compute the SVD to achieve the objective function formula (Eq. (4)) for any candidate plane. Then the objective function can be computed for each triangle of the convex surface. For each triangle, this task is only a matter of evaluating Eq (4). As in the 2D case, only one SVD needs to be performed in order to gain the objective function values for all the triangles. The triangle corresponding to the minimum objective function can then be identified. Then the vertices and edges of that triangle can be checked to see if a plane passing through any of them gives a lower objective function, see Fig. 11(b). The vertices can be checked using the 3D equivalent of the method described above in the 2D case. Each edge can be tested similarly, by rotating the data points such that the edge coincides with the Z-axis, and reducing the problem to a 2D one.

5. Advantages of the constrained least-squares datum

This L2C datum definition with the algorithm shown here has the following advantages:

- The most complex mathematical tools required are a convex hull algorithm and SVD. Both of these are well studied, reliable, and available.
- It can be performed efficiently. In fact, the limiting factor is the convex hull itself for which algorithms exist of time order $n\log(n)$, where n is the number of original points.
- It is not adversely affected by unevenly sampled data points as some datum definitions are.

But the most notable advantage is the remarkable ability of the L2C datum definition that the datum makes full contact with the datum feature when it is stable to do so, and balances rocking conditions when there is instability that requires it.

Figure 12 shows two typical cases where, on the left, one would seek to balance the rocking condition, and on the right, one would seek for the datum plane to be stably flush with the edge of the datum feature. This is what the L2C solution does automatically.

Shakarji, Craig; Srinivasan, Vijay.
"Theory and algorithm for planar datum establishment using constrained total least-squares."
Paper presented at the CIRP Conference on Computer Aided Tolerancing - CAT, Gothenburg, Sweden, May 18-May 20, 2016.

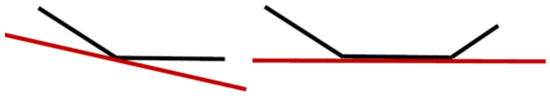


Fig. 12. Two typical cases of datum features with the associated L2C datums shown. The balanced rocking case is on the left and the stable, flush case is on the right.

For the rocker condition pictured on the left side of Fig. 12, if the line segment on the right were made longer, the L2C datum plane would roll to the right smoothly. For the stable case pictured on the right side of Fig. 12, if the line segment on the right were made somewhat longer, the L2C datum plane would not move from its stable state. It would remain flush with the edge of the datum feature until the line segment on the right grew long enough to make a rocker condition, at which point the L2C datum would smoothly begin to roll to the right to balance the rocker.

In contrast, the shifted least-squares solution would achieve a flush mating with the datum feature (as pictured on the right of Fig. 12) for only an instant. That is, as the line segment on the right began to be extended, there would only be one length that resulted in a flush mating. This contrast shows the fascinating feature of the L2C, which stays flush with the datum feature—even while the line segment extends—until it reaches such a length that a rocking condition exists, like shown in Fig. 13.

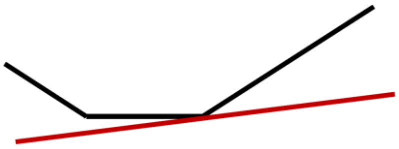


Fig. 13. The line segment on the right is long enough for the constrained L_2 datum to treat it as a rocking condition and separate from the flush contact it had in the right hand picture of Fig. 12.

6. Implementation

The L2C datum definition has been coded and run under various input data set scenarios. The results are that the theory does in fact hold. For 2D, this means that the datum line contacts two points in sufficiently stable cases, and contacts one point when there is a rocking condition, which it appropriately balances. In 3D, the datum plane does, in fact, contact three points in sufficiently stable cases, and contacts two points along an edge, when there is a rocking condition along that edge (which it balances), and contacts one point when there is a rocking condition on that point (which is balanced by this datum plane definition).

7. Conclusion

The L2C datum plane definition automatically shifts between a full-contact solution to stabilizing rocker conditions. Besides other advantages, the definition is robust and, because the nature of the objective function has been investigated in this paper (and in particular because it is convex over the region of interest) reliable, efficient algorithms are available. The mathematical tools required to carry out implementation are reliable and available. Based on all these, the L2C is an attractive choice for standardization of planar datums.

References

[1] Srinivasan, V., "Reflections on the role of science in the evolution of dimensioning and tolerancing standards," Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, Vol. 227, No. 1, pp. 3-11, 2013. DOI: 10.1177/0954405412464012

[2] Tandler, W. "All Those Datum Things" Inside Metrology, Quality Digest, Quality Digest Magazine, 13 February 2008.

[3] Tandler, W. "Establishing Datum Reference Frames," Inside Metrology, Quality Digest, 12 March 2008.

[4] ANSI/ASME Y14.5.1M-2009 "Dimensioning and Tolerancing," The American Society of Mechanical Engineers, New York.

[5] ANSI/ASME Y14.5.1M-1994 "Dimensioning and Tolerancing," The American Society of Mechanical Engineers, New York.

[6] ISO 5459:2011. "Geometrical product specifications (GPS)—geometrical tolerancing—datums and datum systems." Geneva: International Organization for Standardization, 2011.

[7] Zhang, Xuzeng, and Roy, Utpal "Criteria for establishing datums in manufactured parts" Journal of Manufacturing Systems, 12(1), pp 36–50, 1993.

[8] Shakarji, C. M., and Srinivasan V., "Theory and Algorithms for L1 Fitting Used for Planar Datum Establishment in Support of Tolerancing Standards," DETC2013-12372, Proceedings, ASME 2013 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Portland, OR, 2013.

[9] Hopp, T. H., 1990, "The Mathematics of Datums," ASPE Newsletter, September 1990, American Society for Precision Engineering, Raleigh, NC

[10] Shakarji, C. M., and Srinivasan V., "A Constrained L2 Based Algorithm for Standardized Planar Datum Establishment," IMECE2015-51199, Proceedings, ASME 2015 International Mechanical Engineering Congress & Exposition, Houston, TX, 2015.

[11] Horowitz, A., "A version of Simpson's rule for multiple integrals," Journal of Computational and Applied Mathematics 134 (2001) 1–11.

[12] VanHuffel, S., and Vandervalle, J., 1991 The Total Least Squares Problem: Computational Aspects and Analysis, SIAM, Philadelphia, PA.

[13] Shakarji, C. M., and Srinivasan, V., "Theory and Algorithms for Weighted Total Least-Squares Fitting of Lines, Planes, and Parallel Planes to Support Tolerancing Standards," ASME Journal of Computing and Information Science in Engineering, 13(3), 2013.

[14] Shakarji, C. M., and Srinivasan, V., "Datum Planes Based on a Constrained L1 Norm," ASME Journal of Computing and Information Science in Engineering, 15(4), 2015.

[15] Shakarji, C. M., and Srinivasan V., "An improved L1 based algorithm for standardized planar datum establishment," DETC2014-35461, Proceedings, ASME 2014 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Buffalo, NY, 2014.

[16] Trefethen, Lloyd N., and David Bau III. Numerical linear algebra. Vol. 50. Siam 1997. p. 25-31.

Proceedings of the ASME 2016 Manufacturing Science and Engineering Conference
MSEC2016
June 27- July 1, 2016, Blacksburg, Virginia, USA

MSEC 2016-8635

Implementing the ISO 15746 Standard for Chemical Process Optimization

Guodong Shao
Systems Integration Division
National Institute of Standards and Technology
Gaithersburg, Maryland 20899 U.S.A.

Peter Denno
Systems Integration Division
National Institute of Standards and Technology
Gaithersburg, Maryland 20899 U.S.A.

Albert Jones
Systems Integration Division
National Institute of Standards and Technology
Gaithersburg, Maryland 20899 U.S.A.

Yan Lu
Systems Integration Division
National Institute of Standards and Technology
Gaithersburg, Maryland 20899 U.S.A.

ABSTRACT

This paper proposes an approach to integrating advanced process control solutions with optimization (APC-O) solutions, within any factory, to enable more efficient production processes. Currently, vendors who provide the software applications that implement control solutions are isolated and relatively independent. Each such solution is designed to implement a specific task such as control, simulation, and optimization – and only that task. It is not uncommon for vendors to use different mathematical formalisms and modeling tools that produce different data representations and formats. Moreover, instead of being modeled uniformly only once, the same knowledge is often modeled multiple times – each time using a different, specialized abstraction. As a result, it is extremely difficult to integrate optimization with advanced process control.

We believe that a recent standard, International Organization for Standardization (ISO) 15746, describes a data model that can facilitate that integration. In this paper, we demonstrate a novel method of integrating advanced process control using ISO 15746 with numerical optimization. The demonstration is based on a chemical-process-optimization problem, which resides at level 2 of the International Society of Automation (ISA) 95 architecture. The inputs to that optimization problem, which are captured in the ISO 15746 data model, come in two forms: goals from level 3 and feedback from level 1. We map these inputs, using this data model, to a population of a meta-model of the optimization problem for a chemical process. Serialization of the metamodel population provides input to a numerical optimization code of the optimization problem. The results of this integrated process, which is automated, provide the solution to the originally selected, level 2 optimization problem.

INTRODUCTION

Smart Manufacturing Systems (SMS) make a range of planning and control decisions at all levels of the factory hierarchy. Data are critical inputs to, and outputs from, the decision-making process. In fact, according to The Smart Manufacturing Leadership Coalition (SMLC) report on implementing 21st Century Smart Manufacturing [1], large amounts of data must be collected, stored, analyzed, and transmitted across all levels in that hierarchy. The report went on to say that highly efficient, standardized models are needed to manage, integrate, and use that data effectively and affordably.

Today, making planning and control decisions may involve using software tools to formulate and solve multi-criteria optimization problems. Due to the diversity of application environments and the variety of methodologies they implement, however, these tools are often isolated and relatively independent. Because of this, each tool typically requires specialized data formats, and abstractions. This means that, instead of being modeled uniformly once, the same data is often modeled multiple times using different modeling formalisms. Developing, reusing, and integrating the models based on these different formalisms is still a manual, error-prone, and time-consuming activity. The only way to change this situation, as noted in the SMLC report, is to develop standardized data models.

In the process industries, ISO 15519 provides rules and guidelines for representing measurement, control, and actuation

Shao, Guodong; Denno, Peter; Jones, Albert; Lu, Yan.
"Implementing the ISO15746 Standard for Chemical Process Optimization."
Paper presented at the ASME International Manufacturing Science and Engineering Conference (MSEC), Blacksburg, VA, Jun 27-Jul 1, 2016.

in process control diagrams [2]. ISO 10628 defines Piping and Instrumentation Diagrams (P&ID) [5], which capture the functional relationships among piping, instrumentation and system equipment. Several tools are available to create these diagrams. The International Electrotechnical Commission (IEC) 62424 defines procedures and specifications for the exchange of control-relevant data provided by those P&ID tools [3]. ISO 15926 is a standard for data modeling and interoperability that uses several Semantic Web technologies to provide a lifecycle description of a variety of oil, gas, and chemical processes [5].

However, none of these process-related standards addresses the data needed to integrate engineering optimization (O) tools with advanced process control (APC) tools. In this paper, we argue that there are two standards, one accepted and one quite new, that together may provide key to defining and representing that data. Those standards are ISA 95 [5], which does the defining and ISO 15746 [7], which does the representing. We will briefly describe how the ISA 95 hierarchy and its various levels are defined. We then describe how ISO 15746 uses those definitions to develop an interface data model between level 2 and level 3. Next, we describe how we used that data model to develop interfaces between the second and third levels of a process plant implementing a pedagogical chemical process, the Tennessee-Eastman process. We then formulate an optimization problem to demonstrate how the interface actually works using standard Extensible Markup Language (XML) and optimization programming language metamodel. OPLmetamodel is used for the optimization model formulation and IBM CPLEX is used as the optimization solver to solve the problem.

ISA 95

The ISA-95 standard [5] provides a framework for exchanging manufacturing data between hierarchical levels in the factory. Figure 1 shows the high-level functions assigned to each level of that hierarchy. Level 4 defines the business-related activities needed to manage a manufacturing organization. Manufacturing-related activities include establishing the basic plant schedule, determining inventory levels, and making sure that materials are delivered on time to the right place for production. Level 4 determines what and when products are made; it operates on time frames of months, weeks, and days. Level 3 defines the workflow needed to produce the desired end products prescribed in Level 4. For each such product, this flow specifies which physical processes are used and in what order. For each of those processes, Level 3 also specifies the associated recipes. Level 3 typically operates on time frames of days, shifts, hours, minutes, and seconds. Level 2 sets the parameters needed to execute the prescribed workflow/recipes on the selected process. It also monitors and controls that execution. Level 2 typically operates on time frames of hours, minutes, seconds, and sub-seconds. Level 1 defines the activities involved in sensing and manipulating the physical processes. Level 1 provides the data needed for monitoring; it typically operates on time frames of seconds and faster. Level 0 defines the actual physical processes.

In this paper, we explore a novel method of integrating the workflow/recipes and other data from Level 3 with the parameter setting optimization (O) and monitoring/control (APC) in Level 2. That integration is based on data models from a recent standard, ISO 15746. We map information from this data model to a population of a metamodel of optimization problems. Serialization of the metamodel population provides input to a numerical optimization code. Results of the optimization provide the parameter settings, which are the inputs needed for monitoring and control.

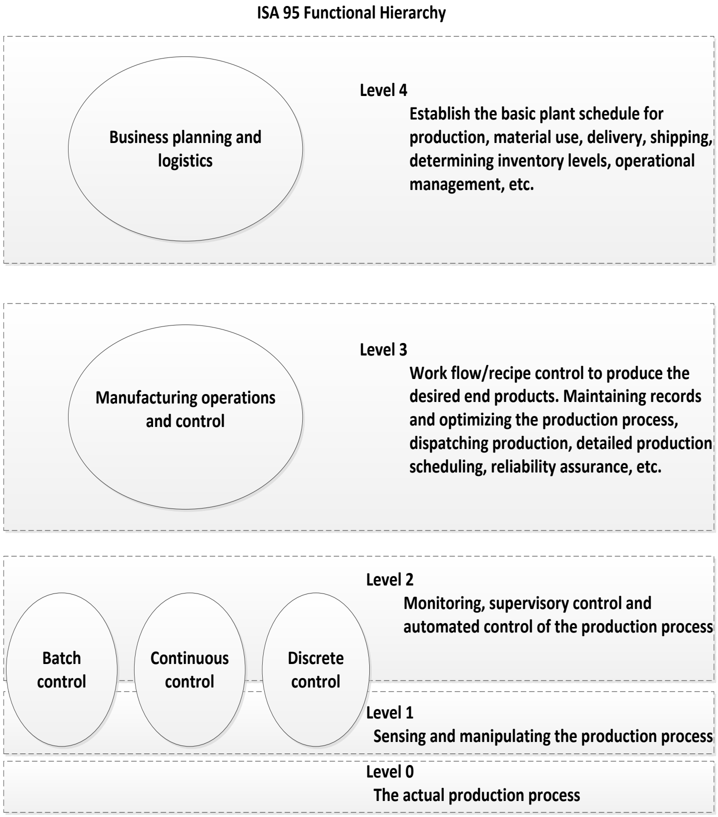

ISA 95 Functional Hierarchy
Business planning and logistics
Level 4
Establish the basic plant schedule for production, material use, delivery, shipping, determining inventory levels, operational management, etc.
Manufacturing operations and control
Level 3
Work flow/recipe control to produce the desired end products. Maintaining records and optimizing the production process, dispatching production, detailed production scheduling, reliability assurance, etc.
Batch control
Continuous control
Discrete control
Level 2
Monitoring, supervisory control and automated control of the production process
Level 1
Sensing and manipulating the production process
Level 0
The actual production process

Figure 1. ISA 95 Levels (ISO 2014)

ISO 15746

The ISO 15746 standard is intended to facilitate the integration and interoperability of software tools that provide automation solutions to optimization and advanced process control (APC-O) problems. Currently, the standard has two parts: ISO 15746-1 [7] and ISO 15746-2 [8]. ISO 15746-1 defines a reference interoperability framework, based on the ISA 95 hierarchy. Its goal is to reduce the cost and risk associated with developing and implementing integrated APC-O tools. Its scope is limited to specifying the set of concepts, terms, definitions, and the associated rules for describing the required functional capabilities of those tools.

The major focus of this paper, however, is on ISO 15746-2, which defines an information model of APC-O to enable integration of different applications and systems. It builds on framework in ISO 15746-1 by defining activity models for APC-O systems and object models for data exchanges to support those activity models. In this paper, we focus on a few information models defined in ISO/CD [8]. Table 1 shows the various symbols used in those models and their definitions.

Figure 2 shows overall structure of the information model starting from the top level as APC-O systems, which is comprised of one or more APC-O Modules [8]. An APC-O Module is identified by Name and Type and may also have one or more vendor-specific attributes that are provided through a discovery service interface. The unique attributes to the type goes into the Vendor-SpecificAttributes section within the module. Every module has an event set and a variable set. Events and variables both have their specific attributes. The top-level diagram defines what types of variables each module has in sets.

Figure 3 shows the information model for APC-OVariable type and the subtypes defined [8]. All APC-O variables Module types have VariableSets of base type APC-OVariable type. VariableSets are sets of variables used by the APC-O system. Defined variable sets are shown for each APC-OModule type. Variables in each of these sets are subtypes of APC-OVariable type, which is an object type defining common attributes of all variables used in APC-O.

Based on ISO 15746-2 [8], there is no generic OptimizationDefinitionType, every optimization tool will need to provide its own unique structure. Figure 4 shows an example of OptimizationDefinition types [8]. It does not represent specific technologies in their entirety but rather illustrate how an integration object might look.

The three instances shown are those that might be of interest external to the specific instantiation of the OptimizationModule.

- A SteadyStateOpt object represents a type of optimization where an objective function is minimized using steady state process models. The path that the process takes to achieve the optimum steady state conditions is not considered.
- A DynamicOpt object represents a type of optimization where an objective function is minimized over a fixed horizon using dynamic process models. Both the path and the final steady state conditions are considered in the solution.
- An ExpertSystemOpt object represents a type of optimization where optimum conditions are determined by a set of rules similar to if-then-else logic. Process models may be embedded in and used by the rules, but these models are not the fundamental basis for determining optimum conditions.

In this paper, we will exemplify the application of standard ISO 15746 using a chemical process, which is a continuous process.

THE TENNESSEE-EASTMAN (TE) CHEMICAL PROCESS

A schematic diagram of the TE chemical process is based on Downs and Vogel [9] as shown in Figure 5. The TE process has five major unit operations: a chemical reactor, a product condenser, a vapor-liquid separator, a product stripper, and a recycle compressor. The process produces two products from four exothermic, irreversible reactions. There are five process inputs labeled as A to E, with component B as an inert, process outputs G and H as the primary products, and process output F as a byproduct.

The gases A to E flowing out of the reactor then go through the condenser. In the condenser, coolant is mixed with cold water and flows through to condense the gas into a liquid. The only measured value is the temperature of the cool water and the only manipulated variable is the cool water flowrate. The remaining gases and liquids are then sent to the vapor liquid separator.

The vapor/liquid separator separates vapor and liquid by using gravity to pull down the liquids into one stream while the gas is taken up to another stream. The measured values for this operation include the separator's pressure, temperature, and level. The only manipulated variable is the flowrate of the liquid leaving the separator. The gas is compressed and sent back to the reactor through the recycle valve. Some of the gas is purged before it gets to the compressor to prevent a buildup. The measured values in this process include the purge stream flowrate, the recycle flowrate, and the work done by the compressor. The manipulated variables include the Purge valve and a recycle valve positions.

The liquid goes into stripper that removes some of the remaining reactants. This is done by sending steam and gas C around the liquid to strip them off the reactants. The measured values are the stripper's pressure, temperature, and level, the steam's flowrate and the underflow rate of the liquid products leaving the scope of the process. The product components, G and H, exit at the stripper base. The inert component, B, and the byproduct component, F, primarily exit the system as vapors from the vapor-liquid separator.

The primary goal of this process is to facilitate a number of reactions. In the expressions that represent the reactions, (g) stands for gas and (liq) stands for liquid. The specific reactions are

A (g) + C (g) + D (g) → G (liq) (the first product) (1)
A (g) + C (g) + E (g) → H (liq) (the second product). (2)

There are also two reactions that create the byproduct liquid F. These reactions are

Table 1 - Information model symbols and definitions

Symbol		Description
Object	object	An object is an item that exists or can exist once constructed, physically or informatically. Associations among objects shall constitute the object structure of the system being modeled, i.e. the static, structural aspect of the system.
▲	aggregation-participation relation link	A fundamental structural relation. Aggregation-Participation is a source item that aggregates one or more other participant items, the destination items, into a meaningful whole.
⟁	Exhibition-characterization relation link	A fundamental structural relation. Exhibition-Characterization means that an item exhibits, or is characterized by, another item. The Exhibition-Characterization relation binds a source item, the exhibitor, with one or more destination items, which shall identify features that characterizes the exhibitor.
△	Generalization-Specialization relation link	Generalization-Specialization relations extend the inheritance concept to both objects and processes. A specialization item has at least the same structural relations and procedural relations as the general item.
◬	Classification-Instantiation relation link	Classification-Instantiation relations connect classes to their instances.

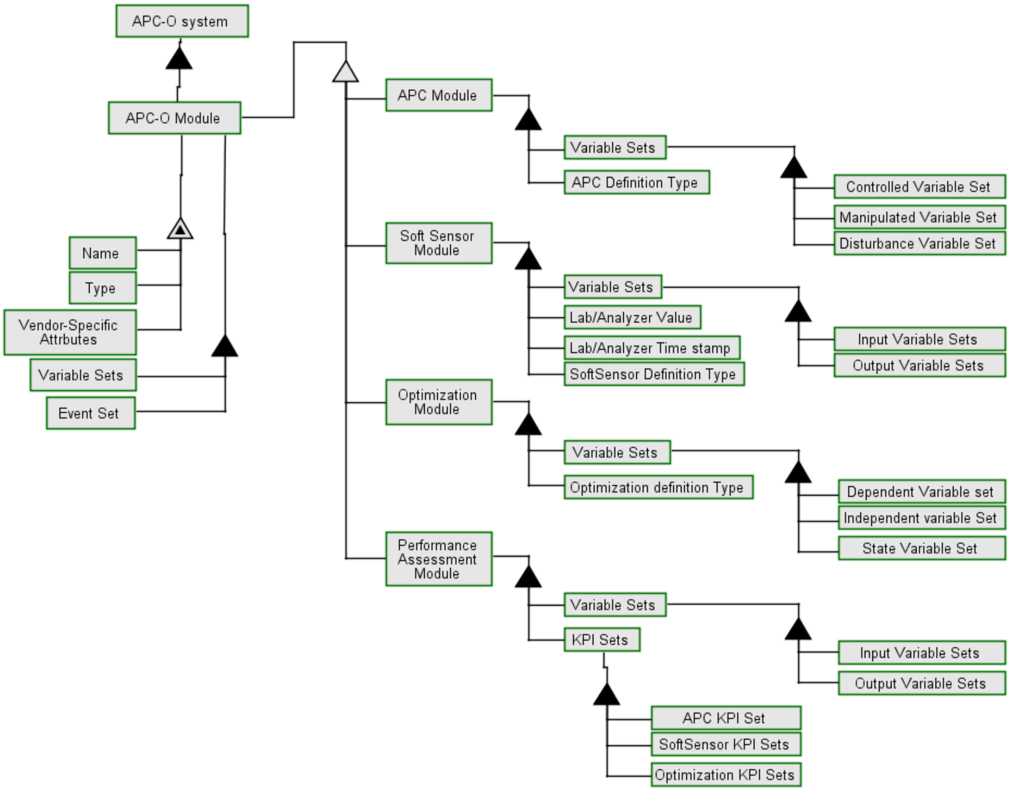


Figure 2. Information model for the APC-O system [8]

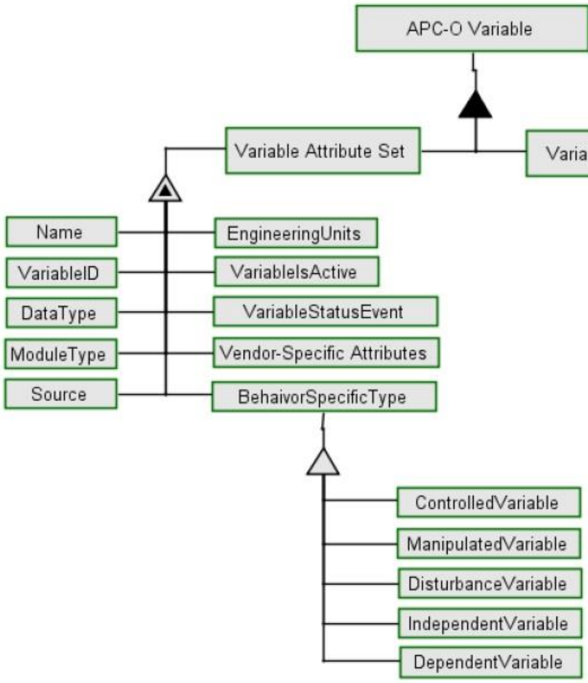


Figure 3. Information model for the APC-O Variable Type [8]

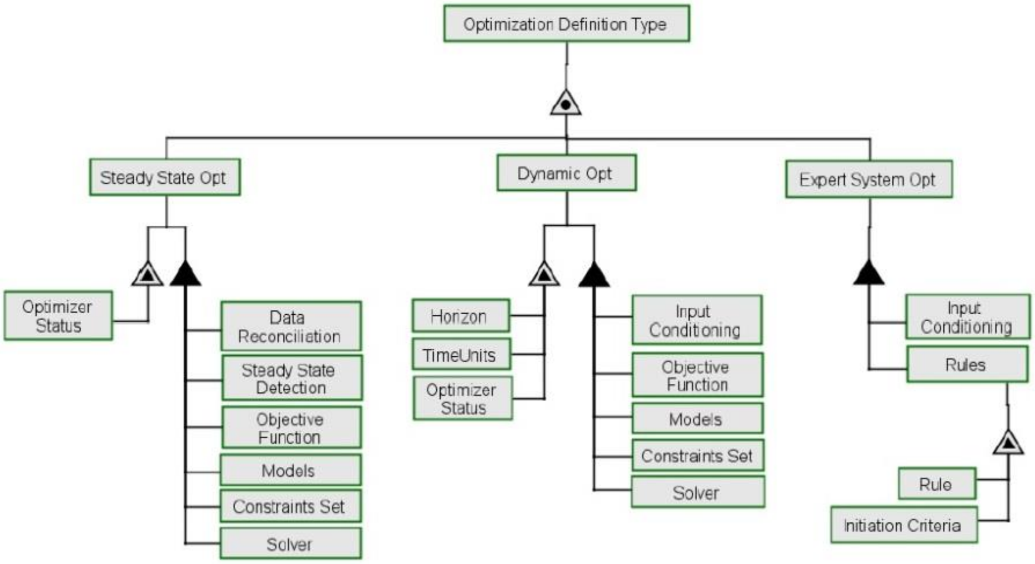


Figure 4. Optimization definition Type [8]

$A(g) + E(g) \rightarrow F(g)$
(3)
$3D(g) \rightarrow F(liq)$.
(4)

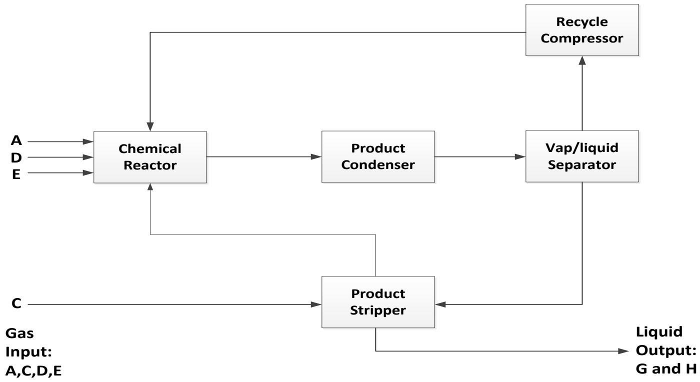


Figure 5. A simplified schematic diagram of the TE chemical process

The reaction rates of the endothermic reaction are a function of heat and reaction is modeled as an ideal, continuous, stirred-tank reactor with internal cooling to remove the heat of reaction. There are 41 measured values in the T-E process and 12 manipulated variables.

HOW TO USE ISO 15746 TO ACHIEVE INTEGRATION

Using ISO 15746 involves a two-stage process. In the development stage (see Figure 6), a conceptual data model provided by the standard is used for specifying corresponding XML schemas. Once created, the XML schemas can be reused for multiple implementations. Any APC-O application can be instantiated based on the schema and the XML data can be exchanged for various uses, including data management, simulation, advanced control and optimization.

In this case, the XML schemas will be used for representing data for the T-E chemical process. Figure 7 and Figure 8 are examples of the created XML schemas.

In the implementation stage, the T-E process is analyzed, equations and relevant data are derived from the MATLAB simulation [10] and literatures [9] [11], data and variables are represented as XML instances according to the developed XML schemas. Then, a subset of those XML instances, related to the optimization problem defined in (see (8) below), is used as input to level 2. Figure 9 is an example of the XML instances. Information from level 2 and level 3 systems is mapped to the optimization metamodel. Those instances are used to create an executable optimization program through the OPLmetamodel.

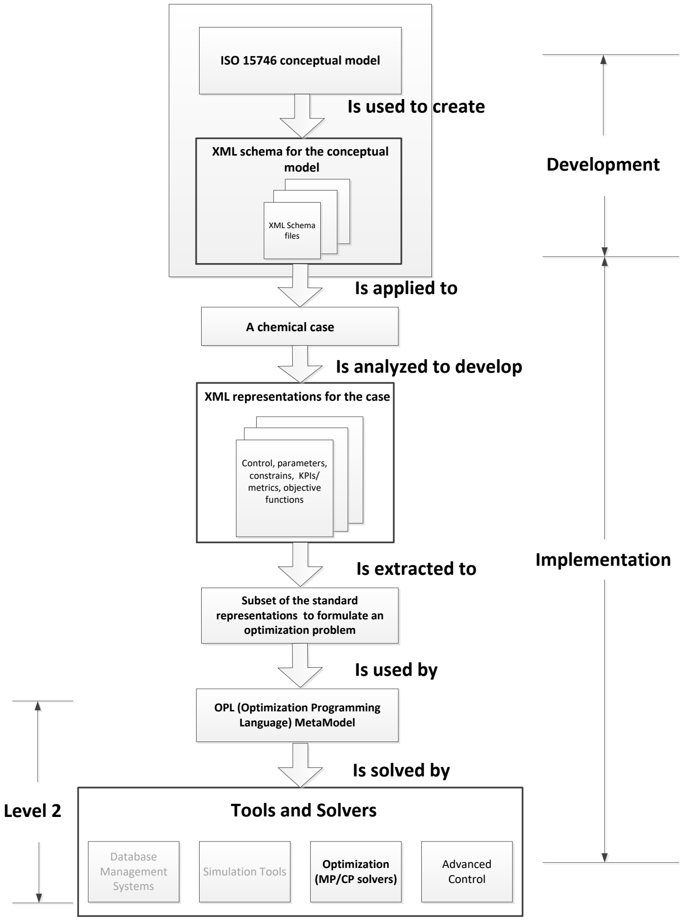

ISO 15746 conceptual model
Is used to create
XML schema for the conceptual model
XML Schema files
Development
Is applied to
A chemical case
Is analyzed to develop
XML representations for the case
Control, parameters, constrains, KPIs/ metrics, objective functions
Is extracted to
Implementation
Subset of the standard representations to formulate an optimization problem
Is used by
OPL (Optimization Programming Language) MetaModel
Is solved by
Level 2
Tools and Solvers
Database Management Systems
Simulation Tools
Optimization (MP/CP solvers)
Advanced Control

Figure 6. Flow of a chemical process optimization based on ISO 15746 standard

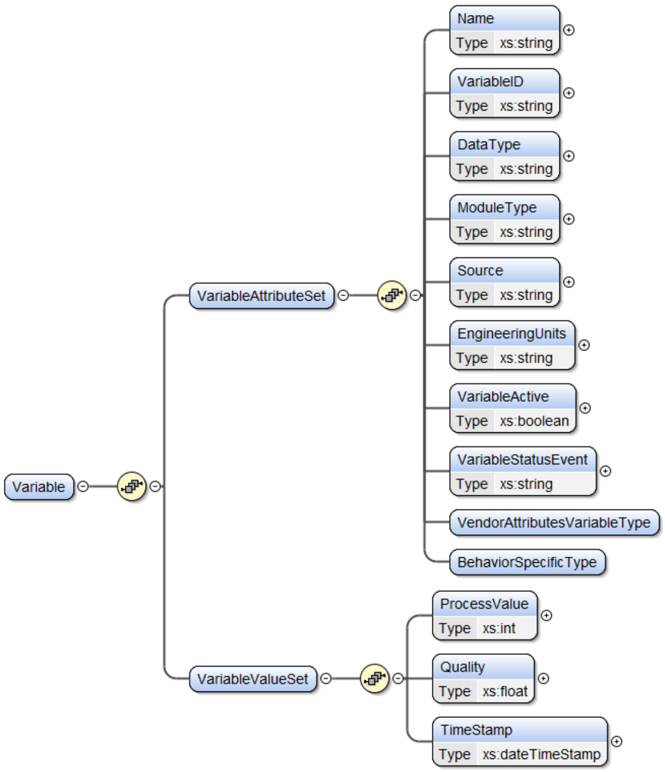


Figure 7. The XML schema for variable

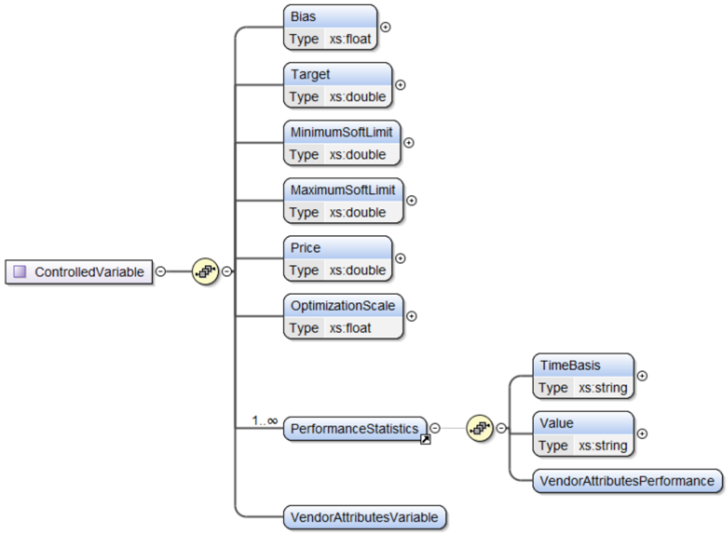
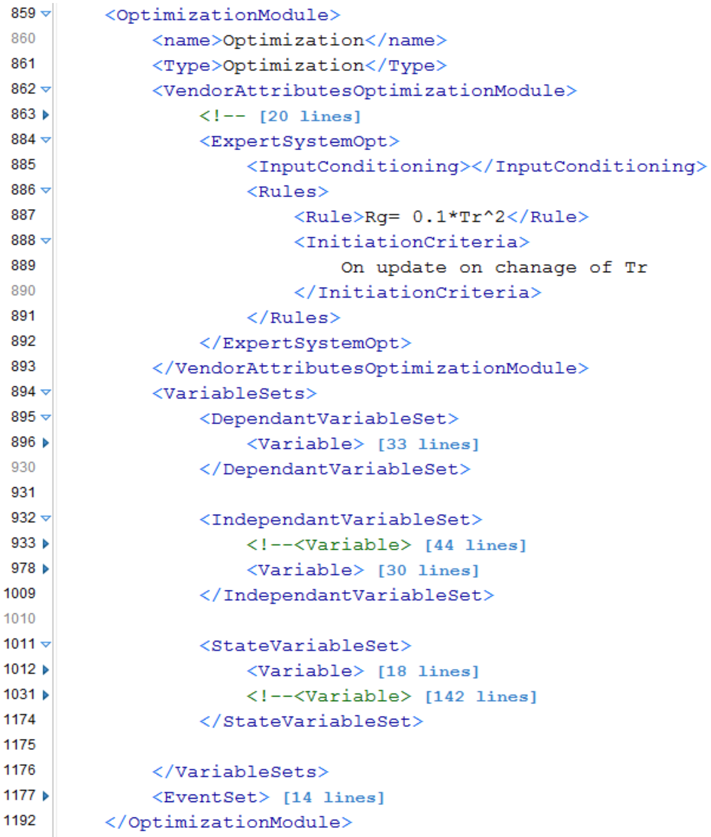


Figure 8. The XML schema for controlled variable



```
<OptimizationModule>
    <name>Optimization</name>
    <Type>Optimization</Type>
    <VendorAttributesOptimizationModule>
        <!-- [20 lines]
        <ExpertSystemOpt>
            <InputConditioning></InputConditioning>
            <Rules>
                <Rule>Rg= 0.1*Tr^2</Rule>
                <InitiationCriteria>
                    On update on chanage of Tr
                </InitiationCriteria>
            </Rules>
        </ExpertSystemOpt>
    </VendorAttributesOptimizationModule>
    <VariableSets>
        <DependantVariableSet>
            <Variable> [33 lines]
        </DependantVariableSet>

        <IndependantVariableSet>
            <!--<Variable> [44 lines]
            <Variable> [30 lines]
        </IndependantVariableSet>

        <StateVariableSet>
            <Variable> [18 lines]
            <!--<Variable> [142 lines]
        </StateVariableSet>

    </VariableSets>
    <EventSet> [14 lines]
</OptimizationModule>
```

Figure 9. A XML instance for the optimization module.

MAPPING THE DATA TO THE OPTIMIZATION METAMODEL

A *metamodel* is a model of a modeling language that provides sufficient detail about the modeling language that it may serve as a storage form for the language. For example, the Unified Modeling Language (UML) metamodel provides description of the concept of things such as classes and methods. Instances of the UML metamodel can describe classes (model content) with sufficient fidelity so that automated tools can generate Java class definitions from the class descriptions.

An optimization metamodel is a conceptual model for capturing, in abstract terms, the essential characteristics of a given optimization problem – such as an objective function and its constraints. The metamodel provides a schema of sufficient formality to enable the problem modeled to be serialized to statements in several, concrete optimization languages – such as the Optimization Programming Language (OPL) [12], A Mathematical Programming Language (AMPL) [13], and the General Algebraic Modeling System (GAMS) [14].

Currently, however, the metamodel developed at the National Institute of Standards and Technology (NIST) only supports OPL [15]. The OPL metamodel specification can be found on the NIST GitHub site [15]. Using that specification, we have developed software to (1) read OPL models and (2) write populations of the metamodel needed to produce complete OPL code for the problems. The purpose of (1) is to produce "templates" for classes of problems. Elements specific to the optimization problem at hand can be substituted for placeholders in the template. The purpose of (2) is, of course, to produce the OPL input for an OPL-capable, numerical optimizer – one of the tools and solvers at the bottom of Figure 6.

An example of usage of the OPLmetamodel in chemical process manufacturing is depicted in Figure 10. The top portion of Figure 10 shows the inputs used in problem formulation (middle layer of Figure 10). Problem formulation concerns the development of design space constraints (typically mathematical inequalities) and objective function (typically an equation with weighted terms). There are many possible technical means of formulating the problem. For this problem, we simply process the XML-based data to expressions of the metamodel and substitute these for elements of the problem template. The completed OPLmetamodel population is then serialized to an optimization solver as depicted in the lower layer of Figure 10.

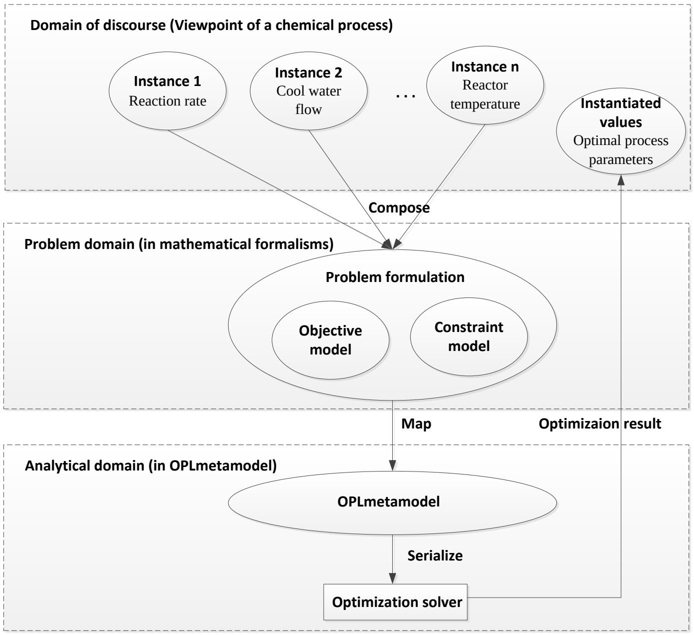


Figure 10. The usage of the OPLmetamodel

EXAMPLE OPTIMIZATION PROBLEM

With the created XML instance files for the case, various analytical and/or control tasks can be modeled and performed. In this section, we demonstrate the model and data transformation using the OPL metamodel, we take a subset of the XML file created for the TE chemical process as input to model a simplified optimization problem. OPLmetamodel is used for the optimization model formulation and IBM CPLEX is used as the optimization solver to solve the problem.

In the chemical case, there are four possible single input single output relationships from manipulated variable to measured value that govern the process: (1) Reactor Cool Water Flow → Reactor Temperature, (2) D-feed Flow → Reactor Level, (3) Separator Pot Liquid Flow → Separator Level, and (4) Product Liquid Flow → Stripper Level. We selected the first set, i.e., Reactor Cool Water → Reactor Temperature relationship as the base of our optimization problem. There is heat generated during the reaction process, so cool water is needed to flow through the reactor to regulate the temperature. Equations and data have been generated and collected by analyzing the corresponding MATLAB simulation program [10]. Particularly, the relationship between manipulated variables and the measured values at Mode 1 has been examined and plotted. The relevant simplified equations are listed below:

$$T_r = -1.85\ C_r + 174.24 \qquad (5)$$

$$R = 0.1 * T_r^2 \quad . \qquad (6)$$

From Equation (5) and (6), we can derive

$$R = 0.1 * T_r^{\ 2} = 0.1*(-1.85*C_r+174.24)^2 \ , \qquad (7)$$

where R: Reaction Rate, T_r : Reactor Temperature, C_r: Reactor Cool Water Flow

To identify the control limits of the valve position, we want to conduct an optimization on the reaction rate (7). In other words, we want to find the value of cool water flow rate that leads to a minimum reaction rate so as to find the lower bound of the valve position of the cool water to avoid that. The constraints of C_r is 13.2 % < C_r < 100 % (out of 227.1 $m^3 h^{-1}$). Therefore, the actual optimization formulation is given by

$$\begin{aligned} \text{Min} \quad & R = 0.1*(-1.85*Cr+174.56)^2 \qquad (8) \\ \text{st} \quad & \\ & Tr = -1.85*Cr+174.56 \\ & 13.27\ \% < Cr < 100\ \% \end{aligned}$$

Figure 11 (at the end of the paper) is a CPLEX execution window that shows the optimization model produced from the optimization metamodel and the optimization result.

We find that the minimum reaction rate is at approximately 94.18 % of the cool water flow. The minimum reaction rate is zero, which means that the reaction stops at this point. The cool water flow valve should be controlled to avoid this cool water flow rate.

SUMMARY AND FUTURE WORK

In conclusion, we developed an approach for using ISA 95 and ISO 15746 (parts 1 and 2) as a foundation for integrating optimization with advanced process control (APC-O) using our recently developed optimization metamodel. We developed XML schemas for the information models defined in the standard, and applied them to a Chemical-processing-plant optimization problem at level 2 of the ISA 95 hierarchy as a demonstration of our approach. That demonstration was based on an OPL metamodel implementation. The OPL metamodel is translated to an OPL model, which is solved directly by a commercial solver, IBM CPLEX.

Future work includes (1) verifying the needs of standard-based modeling and analysis systems by industry and identifying appropriate real world case scenarios, (2) providing feedback to the standards organization responsible for developing ISO 15746, (3) developing metamodels and translators for other numerical solvers, and (4) developing dashboard for automating the modeling formulation and execution.

ACKNOLEDGEMENT

We would like to thank Enan Rahman, a Summer Undergraduate Research Fellowship student, for his help on XML schema development and chemical process analysis and Ibrahim Assouroko for his valuable ideas and discussion.

DISCLAIMER

No approval or endorsement of any commercial product by the National Institute of Standards and Technology is intended or implied. Certain commercial software systems are identified in this paper to facilitate understanding. Such identification does not imply that these software systems are necessarily the best available for the purpose.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. Approved for public release; distribution is unlimited.

REFERENCES

[1] SMLC, 2011, “Implementing 21 Century Smart Manufacturing, Workshop Summary Report,” https://smartmanufacturingcoalition.org/sites/default/files/implementing_21st_century_smart_manufacturing_report_2011_0.pdf

[2] ISO, 2010, 15519-1:2010. “Specification for Diagrams for Process Industry - Part 1: General Rules,” http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37547

[3] ISO, 2014, “ISO 10628-1:2014 Diagrams for the Chemical and Petrochemical Industry - Part 1: Specification of Diagrams,” http://www.iso.org/iso/catalogue_detail.htm?csnumber=51840

[4] IEC, 2014, “IEC 62714 Engineering Data Exchange Format for Use in Industrial Automation Systems Engineering - Automation Markup Language,” http://www.automationml.org/

[5] ISO, 2003, “15926-2: Industrial Automation Systems and Integration - Integration of Life-cycle Data for Process Plants Including Oil and Gas Production Facilities - Part 2: Data Model,” http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29557

[6] ISA, 2014, “ISA-95,” http://www.isa-95.com/

[7] ISO, 2015, “ISO 15746-1: Automation Systems and Integration – Integration of Advanced Process Control and Optimization Capabilities for Manufacturing Systems – Part 1: Framework and Functional Model,” ISO/TC 184/SC5.

[8] ISO/CD, 2015, “ISO TC184/SC 5/WG5 N073. Automation Systems and Integration – Integration of Advanced Process Control and Optimization Capabilities for Manufacturing Systems – Part 2: Activity Models and Information Exchange,” ISO/TC 184/SC5.

[9] Downs, J. J., and Vogel. E. F., 1993, “A Plant-wide Industrial Process Control Problem,” Computers & Chemical Engineering 17(3), pp. 245-255.

[10] ASU, 1998, “Tennessee Eastman Problem for MATLAB,” Arizona State University, http://csel.asu.edu/?q=node/33

[11] Tian, Z., and Hoo K., 2005, “Multiple Model-Based Control of the Tennessee-Eastman Process,” Industrial & Engineering Chemistry Research, 44, 3187-3202, DOI: 10.1021/ie0496939, http://pubs.acs.org/doi/pdf/10.1021/ie0496939

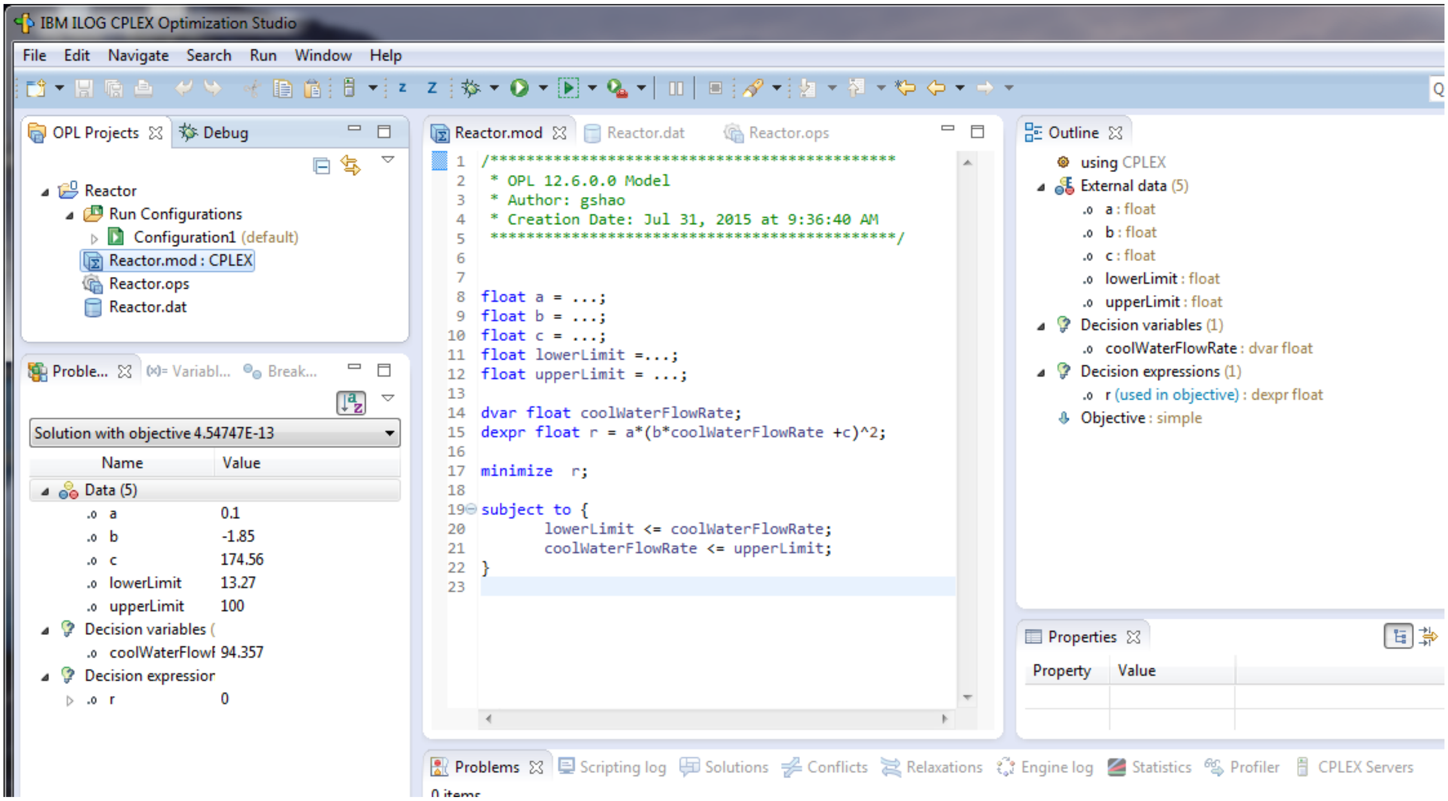
[12] Van Hentenryck P., Lustig I., Michel L., Puget J.F, 1999, “The OPL - Optimization Programming Language,” The MIT Press, Cambridge, Massachusetts, London, England

[13] Fourer R., Gay D.M., Kernighan B.W., 1990, “A Modeling Language for Mathematical Programming,” Management Science, 36, 5, pp. 519-554.

[14] Rosenthal R.E., 2015, “GAMS - A User's Guide,” GAMS Development Corporation, Washington DC.

[15] Assouroko, I., and Denno, P., 2015, “A Metamodel for Optimization Problems,” NIST Interagency/Internal report (NISTIR 8096), Gaithersburg, MD.

[16] NIST., 2015, “NIST Modeling Methodology for Smart Manufacturing Systems,” https://github.com/usnistgov/modelmeth/tree/master/models/optimization



Reactor
- Run Configurations
  - Configuration1 (default)
- Reactor.mod : CPLEX
- Reactor.ops
- Reactor.dat

```
/*********************************************
 * OPL 12.6.0.0 Model
 * Author: gshao
 * Creation Date: Jul 31, 2015 at 9:36:40 AM
 *********************************************/


float a = ...;
float b = ...;
float c = ...;
float lowerLimit =...;
float upperLimit = ...;

dvar float coolWaterFlowRate;
dexpr float r = a*(b*coolWaterFlowRate +c)^2;

minimize  r;

subject to {
        lowerLimit <= coolWaterFlowRate;
        coolWaterFlowRate <= upperLimit;
}
```

Solution with objective 4.54747E-13

Name	Value
Data (5)	
a	0.1
b	-1.85
c	174.56
lowerLimit	13.27
upperLimit	100
Decision variables (	
coolWaterFlowI	94.357
Decision expressior	
r	0

- using CPLEX
- External data (5)
  - a : float
  - b : float
  - c : float
  - lowerLimit : float
  - upperLimit : float
- Decision variables (1)
  - coolWaterFlowRate : dvar float
- Decision expressions (1)
  - r (used in objective) : dexpr float
- Objective : simple

Property	Value

Figure 11. OPL code and CPLEX execution screen

A 3D PRINTING FLEXURE PRESSURE SENSOR FOR ROBOT IMPACT SAFETY TESTING

*Hongliang Shi[1], Yongsik Kim[1], Nicholas Dagalakis[1], Xuechao Duan[2]

[1]Engineering Laboratory, National Institute of Standards and Technology, USA, shi.347@osu.edu

[2]Key Laboratory of Electronic Equipment Structure Design, Xidian University, China

Keywords: 3D printing, pressure sensor, robot safety, flexure structure, stiffness analysis, artifact

Abstract

This paper presents a flexure pressure sensor fabricated by means of 3D printing. This sensor combined with a biosimulant artifact from the National Institute of Standards and Technology (NIST) is used to measure the severity of injuries caused in the case of a robot impact with a human. The stiffness matrix is derived for the structure by means of screw theory. A Finite Element (FE) model is constructed to verify the analytical model and obtain the allowable pressure with regard to the yield stress.

1 Introduction

The movement of manufacturing to countries featuring labor with low hourly wages over the last fifteen years has motivated the development of a new generation of industrial robots that can work side-by-side with human workers [1]. This has created a new technology of Human-Collaboration-Robotics (HCR), which combines the intelligence and dexterity of humans with the strength, repeatability, and endurance of industrial robots [2]. Since most robots are powerful moving machines, the safety of workers working around these robots has become a top priority for safety standards development.

We are using biosimulant materials for the fabrication of inexpensive, disposable HCR safety testing artifacts. These testing artifacts will make possible the measurement of forces, pressure and strain when humans and robots come into contact and also the magnitude of injuries caused by robot static and impact pressure. The Dynamic Impact Testing and Calibration Instrument (DITCI) is a simple instrument, with a significant data collection and analysis capability that is used for the testing and calibration of biosimulant human tissue artifacts [3].

Much work has been done in the design of pressure sensors. Additive manufacturing is widely used for rapid fabrication. Sander et al. [4] designed a monolithic capacitive sensor. Someya et al. [5] designed a flexible pressure sensor matrix for the application of artificial skin. Many Micro-electro-mechanical Systems (MEMS) designs are proposed for pressure sensing [6-12]. However, the costs of these pressure sensors are high. The most common 3D fabrication of polymer objects is fused deposition modeling (FDM). Some other 3D fabrication methods like selective laser melting (SLM), selective laser sintering (SLS), fused filament fabrication (FFF) and stereolithography (SLA) could be used for some other materials or for a higher precision. However, the cost is higher than FDM.

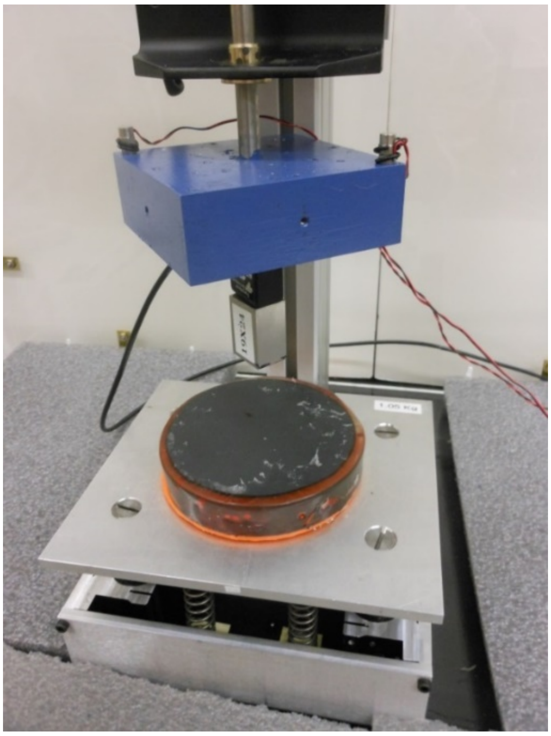


Figure 1. Setting of robot impact testing

In this paper, we propose a structural sensor design, which is mounted underneath the biosimulant artifact. As shown in Fig. 1, the structural sensor mounted under the artifact is set on the DITCI instrument stage. The rest of

Shi, Hongliang; Kim, Yong Sik; Dagalakis, Nicholas; Xuechao, Duan.
“A 3D Printing Flexure Pressure Sensor for Robot Impact Safety Testing.”
Paper presented at the Fifth Asia International Symposium on Mechatronics (AISM 2015), Guilin, Guangxi, China, Oct 7-Oct 10, 2015.

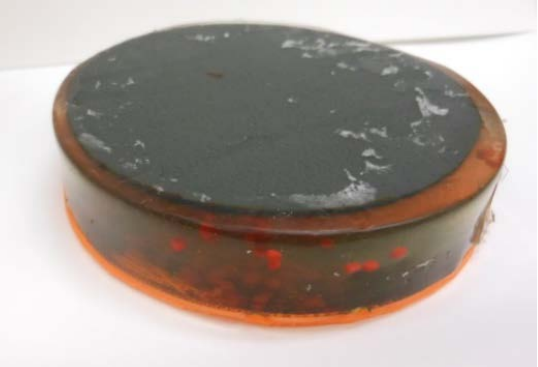
the paper is organized as follows: Section 2 presents the design methodology and fabrication method. Section 3 derives the stiffness matrices for a single pressure cell. Section 4 presents the finite element analysis (FEA) for the design. Section 5 presents the conclusions.

2 Design and fabrication

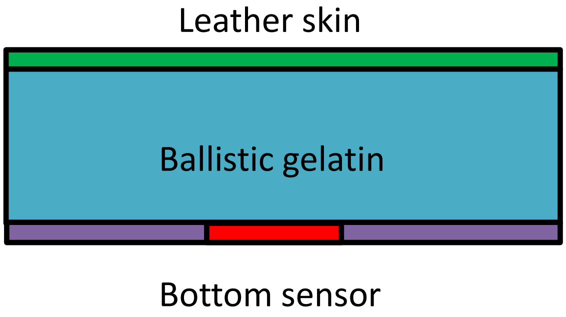
In this section, we describe the design and fabrication of the sensor structure. The sensor system includes a top biosimulant artifact and a bottom sensor. We fabricate the sensor by means of FDM.

2.1 Biosimulant artifacts with bottom sensor

As shown in Fig. 2, the sensor system consists of three layers. The top two layers are called the biosimulant artifact, which consists of disks of biosimulant skin and soft tissue [3]. The bottom layer is the structural sensor.



(a) Artifact with pressure sensor



(b) Schematic drawing of artifact with sensor

Figure 2. Biosimulant artifact and bottom sensor

The biosimulant artifact simulates human skin and muscle and simulates the stress distribution when the impact force is applied on the top of the skin. The bottom structural sensor can measure the pressure on the bottom surface of the ballistic gelatin. By studying the distribution of the stress in the ballistic gelatin caused by the dynamic impact force, we build the relationship of the top impact pressure and the pressure distribution on the bottom surface of the ballistic gelatin. Thus, we are able to reconstruct the top impact pressure from the measurements of the calibrated bottom structural pressure sensor.

As shown in Fig. 3, the bottom sensor has two parts: the center structural sensor and a rigid disk. The white structural sensor will be deformed or destroyed at a certain pressure, while the orange rigid plate has no significant deformation during testing. After each impact testing, the white structural sensor is disposed and it can be replaced for multiple testing with the same biosimulant artifact and plate. This setting is designed to reduce disposable material for lower cost. The size of the white structural sensor should be larger than the tool size. Here, we use a 19 mm × 24 mm tool, as show in Fig. 1. The size of the white structural sensor could be changed based on the application.

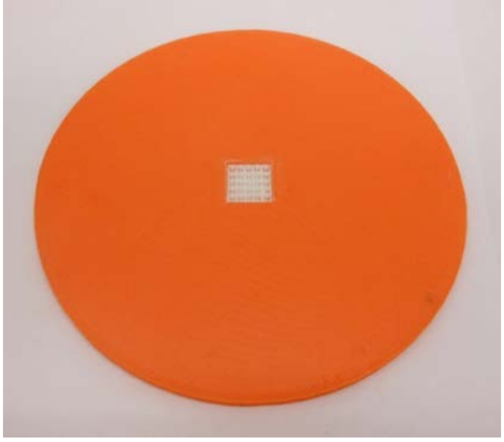


Figure 3. Bottom plate and pressure sensor

2.2 Design of beam based pressure sensor

The structural sensor is shown in Fig. 4. It mainly consists of three parts: top load cube, middle suspending beam, and bottom holding grid. Each top cube is independently supported by the beam. The two ends of each beam are fixed to the bottom grid. The bottom grid structure is designed to be stiff enough so that no deformation occurs when the loading force impacts on the whole structure. A single pressure cell is composed of one top cube, one beam, and bottom grid. Depending on the contact surface of the tool which is creating the impact force, a certain number of the pressure cells are affected so that the cubes will move downwards. Under sufficient pressure, the supporting beam will be destroyed and the top cube will be driven into the grid structure to show an obvious sign of large deformation.

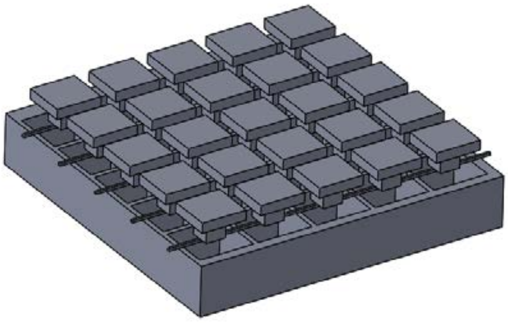


Figure 4. Pressure sensor design

Figure 5 shows a modified design. In this design, the bottom grid has some beams of the grid removed to improve the reliability of the fabrication. Furthermore, the length of each beam is increased to lower the stiffness of the structure. Thus, the allowable pressure can be adjusted. However, the overall size of the sensor is increased.

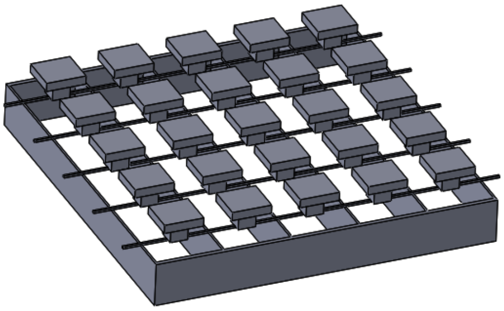


Figure 5. Modified sensor design

2.3 FDM 3D printing fabrication

There are many 3D printers available nowadays. Here, we use a Makerbot Replicator[1] for the fabrication process. As shown in Fig. 6, a single top cubic structure is well printed. The outline is a clear square and there is no extra polymer strings remaining between the squares. We use Makerbot polylactic acid (PLA) as the printing filament material. The printing extrusion and travel speeds are 100 m/s and 45 m/s, respectively. Nozzle temperature is 210 °C and the nozzle size is 0.4 mm in diameter. A well calibrated printer is required to reach the high precision of the printing. Young's modulus of PLA is 3500 N/mm^2 and the yield strength is 45 N/mm^2.

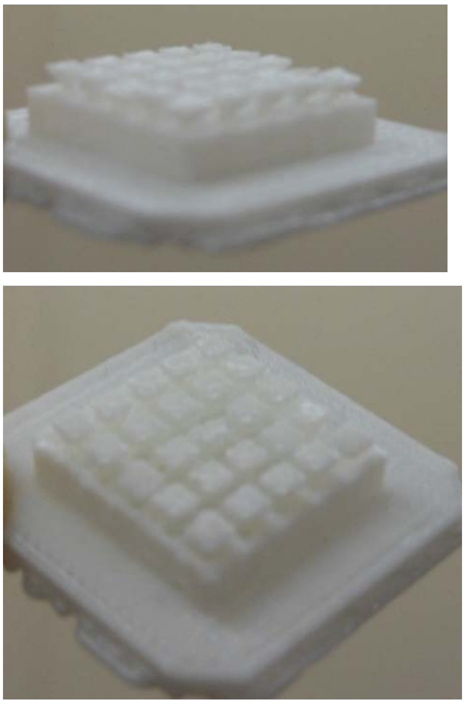


Figure 6. FDM pressure sensor

3 Structural analysis

In this section, the detailed structure of the design is described and later the screw theory based stiffness model is built to calculate the stiffness matrix.

3.1 Design parameters

A schematic drawing of the sensor is shown in Fig. 7. This design is constrained by the capabilities of the 3D printer. With a different type of 3D printing technology, the sensor could be made smaller or from different materials. For example, SLA commonly has a higher resolution and uses cured material like resin.

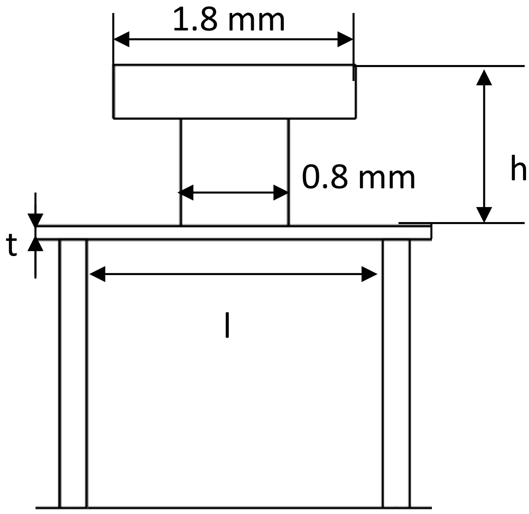


Figure 7. Schematic drawing of sensor

[1] Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

Here, the suspended beam has a rectangular cross section of thickness t and width w. In order to ensure the printing quality, the value of the supporting beams distance l is set as 2.2 mm. A larger l will cause the printed beam to sag, while a smaller l will cause the gap between the top cubes to be too small. Thus, the remaining polymer strings would reduce the quality. The height h is 1.2 mm.

The top cube also has a minimum printable size. If the size is too small, the top could not maintain the square shape. The ideal design is shown in Fig. 7. However, due to the limitation of FDM 3D printing, the actual shape of the printed sensor is shown in Fig. 8. Careful examination of the printed artifact shows that the end of the attachment to the beam center is reduced to a small square. This is because during FDM printing, the filament could not be fully attached to the beam. We take advantage of this phenomenon to create a better design. This design concentrates the applied force on the beam center to increase the free length of the suspending beam. Finally, the beam is easier to deform with the concentrated force loading on its center. Another feature that needs to be assured in the printing is that the two ends of the beam must be fixed on the bottom grid. As is shown in Fig. 8, the two ends of the beam in the actual design extend over the border so that the nozzle will start at the printing position outside the grid.

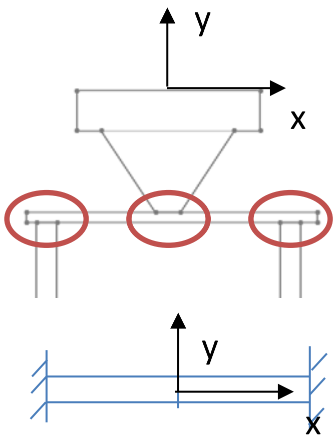


Figure 8. Schematic drawing of FDM sensor

3.2 Stiffness analysis

Here, we adopt the screw theory [13-15] in the analysis of the stiffness matrix. In screw theory, the deformation is denoted by a general twist vector $T = (\theta_x, \theta_y, \theta_z, \delta_x, \delta_y, \delta_z)$ and the loading is denoted by a wrench vector $W = (F_x, F_y, F_z, M_x, M_y, M_z)$. The stiffness matrix is defined *as* $W = [K]T$. Here, the units of the rotational and translational displacement are radian and millimeter, respectively. The units of force and moment are Newton and Newton-millimeter, respectively.

In the stiffness modeling of the sensor structure, we split the beam to two segments from the center plane of the beam. The two segments are considered to be connected in parallel [16-17]. The stiffness of a single beam with rectangular cross section is

$$[K_b] = \frac{EI_z}{l}\begin{bmatrix} 0 & 0 & 0 & \frac{12}{l^2\eta} & 0 & 0 \\ 0 & 0 & -\frac{6}{l} & 0 & \frac{12}{l^2} & 0 \\ 0 & \frac{6}{l\kappa} & 0 & 0 & 0 & \frac{12}{l^2\kappa} \\ \chi\beta & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{4}{\kappa} & 0 & 0 & 0 & \frac{6}{l\kappa} \\ 0 & 0 & 4 & 0 & -\frac{6}{l} & 0 \end{bmatrix}, \qquad (1)$$

where $\eta = t^2/l^2$, $\kappa = I_z/I_y = t^2/w^2$, $\chi = 1/2(1+\upsilon)$, υ is the Poisson's ratio 0.3 and β is derived from

$$\beta = 12\left(\frac{1}{3} - 0.21\frac{t}{w}\left(1 - \frac{1}{12}\left(\frac{t}{w}\right)^4\right)\right). \qquad (2)$$

Through an adjoint transformation matrix $[Ad]$, we could derive the stiffness of the mechanism by means of the equation

$$[K] = [Ad_1][K_w][Ad_1]^{-1} + [Ad_2][K_w][Ad_2]^{-1} \qquad (3)$$

where $[Ad_1]$ and $[Ad_2]$ are defined by

$$[Ad] = \begin{bmatrix} R & 0 \\ DR & R \end{bmatrix} \qquad (4)$$

Here, $[D]$ is the skew-symmetric matrix defined by the translational vector d [12-13].

$$[R_1] = [X(0)]\; d_1 = (0, h, 0). \qquad (5)$$

$$[R_2] = [Z(\pi)]\; d_2 = (0, h, 0). \qquad (6)$$

The subscript 1 means left half segment beam and 2 means right half segment beam. After substituting for the material property of PLA, we could obtain the stiffness matrix as

$$[K]=\begin{bmatrix} 0 & 0 & -76.36 & 63.63 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.52 & 0 \\ 0.63 & 0 & 0 & 0 & 0 & 0.52 \\ 0.79 & 0 & 0 & 0 & 0 & 0.63 \\ 0 & 0.21 & 0 & 0 & 0 & 0 \\ 0 & 0 & 91.85 & -76.36 & 0 & 0 \end{bmatrix} \quad (7)$$

The value 0.52 N/mm is the required force in the y direction for a 1 mm translational displacement.

4 Verification via finite element analysis

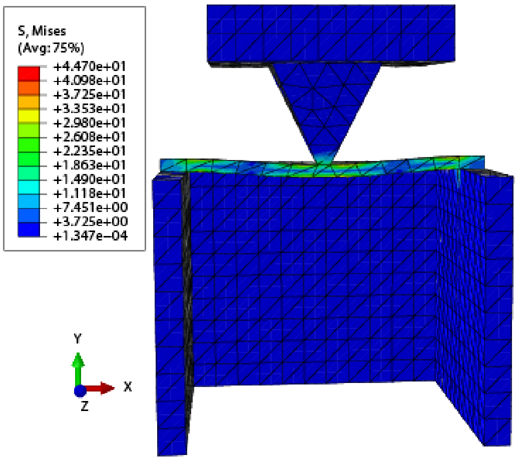


Figure 9. The FE model of a single pressure cell

In order to verify the derivation of the stiffness matrix, we conduct the finite element analysis for the single pressure cell. As shown in Fig. 9, we build the FE model in Abaqus with 4502 elements. The structure is fixed at the bottom and pressure is applied on the top surface. When the maximum Von Mises stress reaches the yield stress of 45 N/mm^2, we record the corresponding loading force and displacement. The top cube moved 0.056 mm downwards with a loading force 0.028 N. The loading force is evenly distributed on the top surface to form the pressure loading.

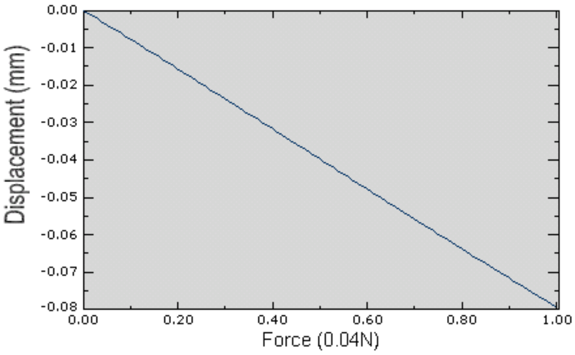


Figure 10. Force vs displacement in the y direction

According to the coordinate frame of Fig. 9, we present the relationship of the force and the displacement in the y direction. As shown in Fig. 10, the beam deforms linearly with respect to the loading. After fitting the points by means of the least squares method, we obtain the value of the stiffness 0.5 N/mm, which is close to the values derived from the stiffness matrix in Eq. 7.

5 Conclusions

This paper presents a structural pressure sensor design fabricated by means of 3D printing. Some meaningful conclusions can be drawn as following.

(1) The structural pressure sensor is disposable, low cost, and easy to fabricate.

(2) We derived the stiffness matrix for a single pressure cell by means of screw theory.

(3) From the result of the FE model, we obtain the loading force 0.028 N. By changing the area of the top surface, we could control the allowable failure pressure.

Acknowledgment

This work was supported by the Robotic Systems for Smart Manufacturing Program of the Intelligent Systems Division, Engineering Laboratory, National Institute of Standards and Technology, USA.

References

[1] Guizzo, E., and Ackerman, E., “How Rethink Robotics Built Its New Baxter Robot Worker,” IEEE Spectrum, 2012,

[2] Pine, A., “Just Ahead: The Robotics Revolution,” Kiplinger Magazine, Jan. 8, 2013

[3] Dagalakis, N.G., Yoo, J.M., and Oeste, T., “Human-Robot Collaboration Dynamic Impact Testing and Calibration Instrument for Disposable Robot Safety Artifacts”, under review.

[4] Sander, C.S., Knutti, J. W., and Meindl, J., “A Monolithic Capacitive Pressure Sensor with Pulse-Period Output”, IEEE Transactions on Electron Device, 1980, 27, (5).

[5] Someya, T., Sekitani, T., Iba, S., Kato, Y., Kawaguchi, H., and Sakurai, T., “A large-area, flexible pressure sensor matrix with organic field-effect transistors for artificial skin applications,” PNAS, 2004, 101, (27), pp. 9966-9970.

[6] Shi, H., Duan, X. C., and Su, H-J. “Workspace optimization of a MEMS hexapod nanopositioner using an adaptive genetic algorithm,” 2014 IEEE International Conference on Robotics and

Automation, (ICRA2014), Hong Kong, May 31-June 7, 2014, pp4043-4

[7] Shi, H., Su, H.-J., and N. Dagalakis, “A stiffness model for control and analysis of a MEMS hexapod nanopositioner”, Mechanism and Machine Theory, 2014, 80, pp. 246-264.

[8] Shi, H., Su, H.-J., Dagalakis, N., and Kramar, J. A., “Kinematic modeling and calibration of a flexure based hexapod nanopositioner,” Precision Engineering, 2013, 37, (1), pp. 117 – 128.

[9] Abeysinghe, D. C., Dasgupta, S., Boyd, J. T., and Jackson, H. E., “A Novel MEMS Pressure Sensor Fabricated on an Optical Fiber”, IEEE Photonics Technology Letters, 2001, 13, (9).

[10] Palasagaram, J. N. and Ramadoss, R., “MEMS - Capacitive Pressure Sensor Fabricated Using Printed-Circuit-Processing Techniques”, IEEE Sensors Journal, 2006, 6, (6).

[11] Krondorfer, R. H., and Kim, Y. K., “Packaging Effect on MEMS Pressure Sensor Performance”, IEEE Transactions on Components and Packaging Technologies, 2007, 30, (2).

[12] Nakamura, K., Iwasaki T. Yamakawa T., and Onishi K., “MEMS pressure sensor”, US Patent, no. 8516905 B2.

[13] Su, H.-J., Shi, H., and Yu, J. “A symbolic formulation for analytical compliance analysis and synthesis of flexure mechanisms,” ASME Journal of Mechanical Design, 2012, 134, (5), pp. 051009-1-9

[14] Shi, H., “Modeling and analysis of compliant mechanisms for designing nanopositioners,” Ph.D. dissertation, OSU, Columbus, MD, 2013.

[15] Su, H.-J., Shi, H., and Yu, J., “Analytical compliance analysis and synthesis of flexure mechanisms,” in Proceedings of ASME IDETC/CIE, Washington, DC, August 28-31, 2011.

[16] Shi, H. and Su, H.-J., “An analytical model for calculating the workspace of a flexure hexapod nanopositioner,” ASME Journal of Mechanisms and Robotics, 2013, 5, (4), p. 041009.

[17] Shi, H. and Su, H.-J., “Workspace of a flexure hexapod nanopositioner,” in Proceedings of ASME IDETC/CIE, 2012, Chicago, Illinois, August 12-15.

BIOSIMULANT ARTIFACT WITH EMBEDDED CALCIUM ALGINATE BEAD SENSOR FOR ROBOT IMPACT SAFETY TESTING

Hongliang Shi[1], Nicholas G. Dagalakis[2]
[1]**Former Research Associate in National Institute of Standards and Technology**
Gaithersburg, MD 20899, USA
shi.347@osu.edu
[2]**National Institute of Standards and Technology**
Gaithersburg, MD 20899, USA
nicholas.dagalakis@nist.gov

ABSTRACT

This paper presents the design of a disposable biosimulant human tissue artifact system for robot safety testing. It is used to provide a visual indication of potentially severe injuries caused in the case of a robot impact with a human. The fabrication method is described including the design and fabrication of the calcium alginate bead and the embedding procedure of the beads into the biosimulant artifact. The artifact system is tested with a Dynamic Impact Testing and Calibration Instrument (DITCI) from the National Institute of Standards and Technology (NIST). The design is useful for the preparation of new robot safety standards.

INTRODUCTION

The movement of manufacturing to countries featuring labor with low hourly wages over the last fifteen years has motivated the development of a new generation of industrial robots that can work side-by-side with human workers [1]. This has created a new technology of Human-Collaboration-Robotics (HCR), which combines the intelligence and dexterity of humans with the strength, repeatability, and endurance of industrial robots [2]. Since most robots are powerful moving machines, the safety of workers working around these robots has become a top priority for safety standards development. We are using biological simulant (biosimulant) materials for the fabrication of inexpensive, disposable HCR safety testing artifacts. These testing artifacts will make possible the measurement of forces, pressure, and strain when humans and robots come into contact as well as of the magnitude of injuries caused by robot static and impact pressure. The Dynamic Impact Testing and Calibration Instrument (DITCI) is a simple instrument shown in Figure 1, with a significant data collection and analysis capability that is used for the testing and calibration of biosimulant human tissue artifacts [3, 4].

Various research groups have used human subjects to collect data on pain induced by the clamping force, pressure, and maximum impact force of the HCRs [5, 6, 7, 8]. Although the results of these tests are hard to reproduce and can vary even among subjects of similar characteristics, they can be very useful for the preparation of safety testing standards. Unfortunately, human safety testing is not an option for HCR industrial applications every time there is a change of a tool or control program, so the use of a biosimulant artifact system is expected to be a good alternative.

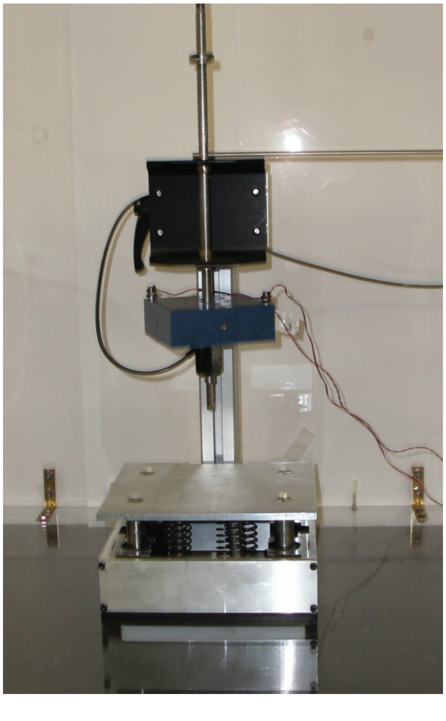


FIGURE 1. Impact testing set up.

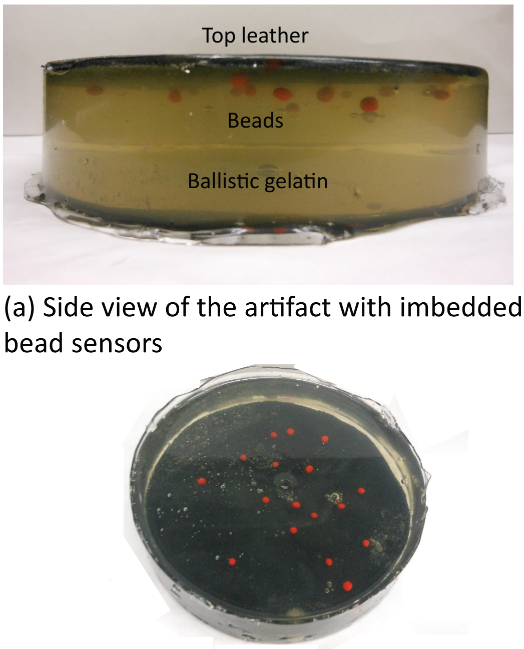
Much work has been done in the design of pressure sensors. Sander et al. [9] designed a monolithic capacitive sensor. Someya et al. [10] designed a flexible pressure sensor matrix for the application of artificial skin. A number of Microelectro-mechanical Systems (MEMS) designs are proposed for pressure sensors [11, 12, 13, 14]. However, the cost of these pressure sensors is high. Based on a chemical fabrication method, we could build a cheap and disposable measurement system. Daly and Knorr [15] proposed the fabrication of a chitosan alginate capsule. Huguet and Dellacherie [16] described the fabrication of calcium alginate beads coated with chitosan.

In this paper, we present a chemical based fabrication procedure for a disposable human artifact embedded with calcium alginate bead for robot impact safety testing. The rest of the paper is organized as follows: We firstly present the design methodology of the artifact system. Secondly, the fabrication method of the calcium alginate bead is followed by a description of the procedure for embedding the beads into the human tissue artifact. Finally, the biosimulant artifact system is mounted on the DITCI for an impact testing.

DESIGN OF BIOSIMULANT ARTIFACT WITH EMBEDDED BEAD

In this section, we describe the design of the biosimulant artifact system. As shown in Figure 2, the sensor system consists of three parts: top leather, soft tissue, and embedded sensor. The top leather is a piece of artificial skin of disk shape. Soft tissue is made of ballistic gelatin. The embedded sensor is a calcium alginate-based bead design. The combination of top leather and ballistic gelatin is called the biosimulant artifact [3].

The biosimulant artifact simulates human skin and muscle, and simulates the stress distribution when the impact force is applied on the top surface of the skin. The deformation of the ballistic gelatin caused by the dynamic impact force results in the stress distributed on the bead sensors. Thus, the embedded bead sensors will deform corresponding to the deformation of the ballistic gelatin. When the red beads over-deform, they will be destroyed when the impact force causes a certain pressure threshold to be exceeded. Due to the low fabrication costs, the artifact may be disposed of after testing.



(a) Side view of the artifact with imbedded bead sensors

(b) Bottom view of the biosimulant artifact system

FIGURE 2. Biosimulant artifact and embedded sensor.

FABRICATION OF CALCIUM ALGINATE BEAD

In this section, we present the fabrication of the calcium alginate bead. The main chemical reaction is based on the mixing of a solution of sodium alginate and calcium chloride. As shown in Figure 3, there are two solutions: base and bath. The base solution is used to drop into the bath solution. Here, the base solution is sodium alginate and the bath solution is calcium chloride.

The base solution consists of sodium citrate, deionized (DI) water, latex, and sodium alginate. The chemicals used in the fabrication are shown in Table 1. Firstly, sodium citrate is dissolved in the DI water to obtain a transparent solution. The sodium citrate is used to remove the calcium ions which will otherwise react with the sodium alginate. Then, red latex enamel is added into the solution. By stirring with a steel stick, we can obtain a red solution without the calcium ion. Finally, we add sodium alginate. Stirring the sodium alginate solution continues until the sodium alginate powder is fully dissolved. This takes approximately 15 minutes. The bath solution is obtained by dropping calcium chloride into DI water. The materials used in fabrication of the artifacts are food-grade, making them easy to procure and use. Sodium citrate, sodium alginate, and calcium chloride are purchased from Modernist Pantry [1]. The latex

[1] Certain commercial materials, equipment, and instru-

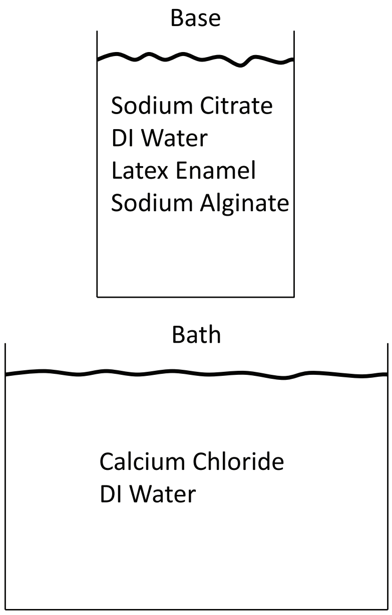


FIGURE 3. Preparation of the base and bath.

enamel of gloss cherry is from Valspar.

As shown in Figure 4, the base is dropped into the bath with a pipette. The viscosity of the base should be higher than the one of the bath so that the drop of the base maintains the original shape of the beads instead of dispersing. If the viscosity is not high enough, xanthan gum could be added to the base to make the solution stickier.

The pipette is positioned at a height shown in Figure 4 to ensure the drop can maintain its shape when it contacts the surface of the bath solution. We can continue dropping several drops, but each drop needs to be kept at some distance from the rest so that they do not stick to each other. The beads are kept in the bath for 2 minutes. In this step, the sodium alginate in the base attracts the calcium chloride in the bath. This reaction creates one layer of calcium alginate as shown in Figure 4. The calcium alginate is a kind of membrane which surrounds the inside liquid sodium alginate. After we take out the beads from the bath and soak them in the DI water, we manually stir the water for about 2 minutes to clean the remaining calcium chloride on the outside surface of the membrane. In this step, if the beads are kept over 30 minutes in the DI water, the size of the beads will increase because the calcium alginate membrane is porous and the DI water is absorbed by the beads.

Finally, we take the beads out of the DI water. Instead of drying the beads, we keep them wet and store in the refrigerator. The extra calcium ions in the outside membrane will keep reacting with the inside liquid sodium alginate. After about 12 hours, the bead turns to be a uniform ball, which contains water like a sponge.

TABLE 1. Chemicals of sodium alginate bead.

Chemical	Quantity (g)	Testing (g)
Sodium citrate	0.1	0.15
DI water	10	10.25
Latex enamel	2	2
Sodium alginate	0.08	0.08
Calcium chloride	0.2	0.2
DI water	20	20.6

FABRICATION OF BIOSIMULANT ARTIFACT AND EMBEDDING PROCEDURE OF BEAD

Our current artifact consists of a disk of biosimulant skin and the soft tissue shown in Figure 2. In nature, human skin consists of a thin outer layer called the epidermis, a thick inner layer called the dermis, and subcutaneous fat. The skin is the first layer of defense against impact injuries, which have been studied by medical professionals and forensic researchers. Because cadavers are expensive and difficult to maintain, forensic researchers have been searching for biosimulant materials with mechanical properties similar to those of human skin [17]. There are a few suppliers of this type of material. For all of our artifact test samples, we used chromed tanned cowhide, Full Cowhide Side, Upholstery or Garment Leather Black [18]. Its thickness is about 1.1 mm and it well simulates the human skin of the mechanical property.

Water solutions containing 10 % to 30 % mass of gelatin have been studied extensively and are considered to be good human muscle tissue biosimulants [19]. Here are the most important conclusions relevant to our work. For nonpenetrating injuries, a water solution containing 20 % mass of gelatin gives a better representation of muscle tissue impact response [20], since the muscle tissue is compressed. For penetrating injuries, a water solution containing 10 % mass of gelatin is more appropriate [21], since the muscle tissue is teared. Distilled water should be used for the gelatin solutions to avoid contami-

ments are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

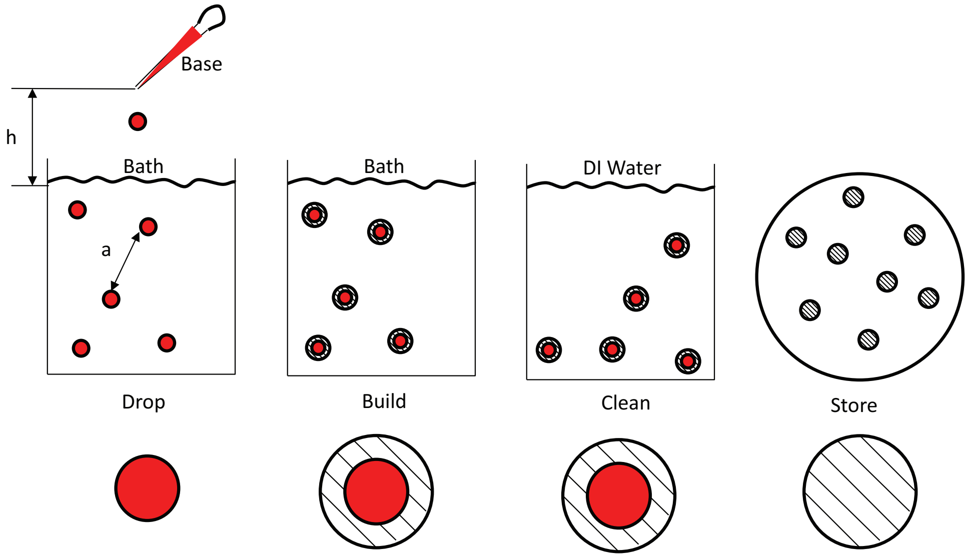


FIGURE 4. Fabrication of the calcium alginate beads.

nants and acidity variations [22]. For all of our test artifact preparations, we used a distilled water solution containing 10% mass gelatin powder supplied by Vyse Professional Grade Ballistic & Ordnance Gelatin [23].

As shown in Figure 5, the solution is poured on top of the skin-biosimulant in an aluminum or glass mold. The glass mold produced artifacts of excellent transparency, and are preferred over the metal molds. The gelatin forms a strong bond with the back side of the skin biosimulant and is observed never to delaminate during impact tests.

After pouring the first layer of ballistic gelatin, we drop the beads into the liquid gelatin. The beads will float due to their light weight. In order to seal the beads, the liquid gelatin need to be cured. The curing process could be accelerated by placing the gelatin in the refrigerator. When the first layer of the gelatin is partially cured, we pour the liquid gelatin for the second layer. Once the second layer of gelatin is fully cured, the embedding procedure is completed. The most important thing in embedding is the temperature control of the first and second layer of gelatin. The first layer of gelatin needs to be cool enough in order to seal the beads. The temperature of the poured liquid gelatin for the second layer needs to be around 30 degree Celsius. If the temperature is too high, the gelatin will heat up the contact surface of the first layer of gelatin. This results in releasing the sealed beads, which will float to the top surface of the second layer of gelatin. If the temperature is too low, the bonding of the first and second layer will be not strong enough to remain bonded throughout the impact testing.

As shown in Figure 5, we take out the artifact system from the mold after the ballistic gelatin is fully cured. The height of the artifact corresponds to the thickness of human tissue. In this paper, the height of the used artifact was 5 cm (4”) because it simulates the soft tissue of the human abdomen. The beads need to be sealed in the gelatin because they are porous and contain water. If the beads dry out, their behavior becomes rubber-like.

IMPACT TESTING

In this section, we demonstrate the artifact system in the robot impact testing device, shown in Figure 1. The fabrication parameters of the sample bead are shown in Table 1. The tool attached to the weight drops on the artifact. This simulates the impact on the human abdomen.

As shown in Figure 6, the tool hits the leather first, and then deforms the gelatin and the embedded red bead. Here, we use a tool with a cross section of 5 mm × 6 mm. The force sensor fixed on the tool records a maximum value of 118 N. Thus, the corresponding pressure is 3.93 N/mm^2, which is higher than the the maximum allowable transient pressure, 2.86 N/mm^2[24]. No tearing is observed. This means that the tool has gen-

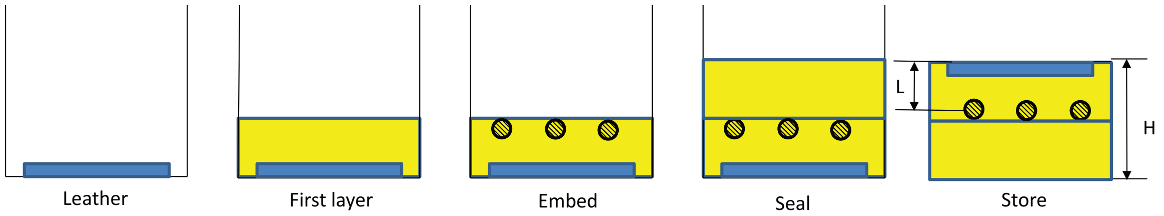


FIGURE 5. Embedding procedure of the beads into the biosimulant artifact.

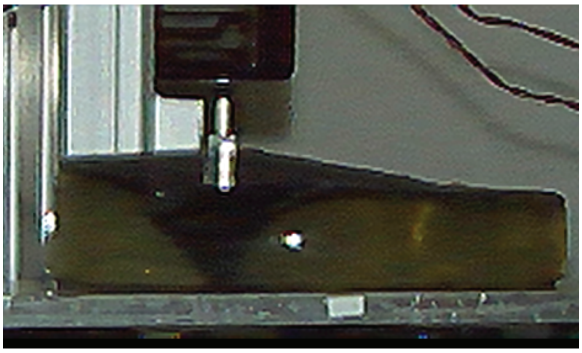


FIGURE 6. Impact testing of bead sensor embedded artifact system.

erated a serious abdominal injury. Figure 7 (a) shows the original embedded bead sensor. Figure 7 (b) shows the destroyed bead after the impact testing.

After we section the ballistic gelatin, we can see the destroyed bead sensor in Figure 7 (c).

CONCLUSION

In this paper, a design of a disposable low-cost biosimulant human tissue artifact system is proposed. It is used for the measurement of the injuries caused by a robot impact force. The fabrication and embedding procedure of calcium alginate bead senors are described. In the impact testing, the bead is destroyed and shows a clear sign that the tool hit the artifact severely. This design can be used in the preparation of artifact safety test standards.

ACKNOWLEDGMENT

This work was supported by the Robotic Systems for Smart Manufacturing Program of the Intelligent Systems Division, Engineering Laboratory, National Institute of Standards and Technology, USA.

REFERENCES

[1] Guizzo E, Ackerman E. How Rethink Robotics Built Its New Baxter Robot Worker, IEEE Spectrum; 2012.

[2] Pine A. Just Ahead: The Robotics Revolution; Jan 8, 2013.

[3] Dagalakis NG, Yoo JM, Oeste T. Human-Robot Collaboration Dynamic Impact Testing and Calibration Instrument for Disposable Robot Safety Artifacts. Industrial Robot: An International Journal;Accepted.

[4] Shi H, Kim Y, Dagalakis N, Duan X. A 3D printing flexure pressure sensor for robot impact safety testing. In: The Fifth Asian International Symposium on Mechatronics (AISM). Guilin, China; 2015. Forthcoming.

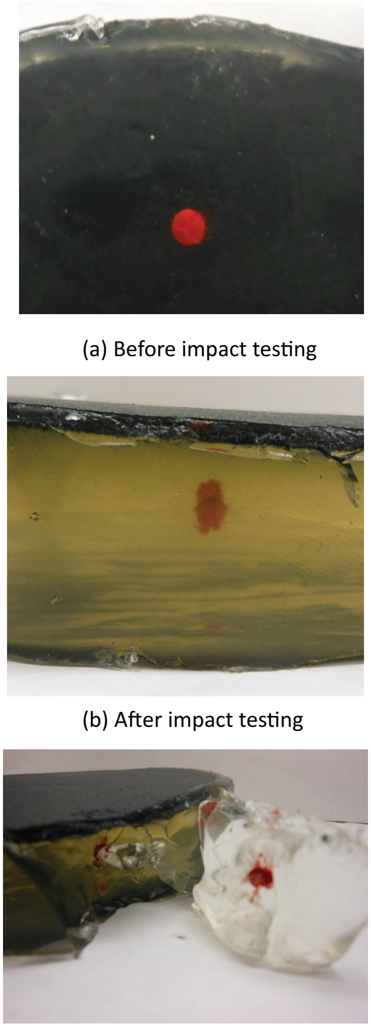
[5] Robots for Industrial Environments: Safety Requirements. Part1: Robot, ISO 10218-1:2011; 2011.

[6] Haddadin S, Albu-Schaffer A, De Luca A, Hirzinger G. Collision detection and reaction: A contribution to safe physical Human-Robot Interaction. In: Intelligent Robots and Systems, 2008. IROS 2008. IEEE/RSJ International Conference on; 2008. p. 3356–3363.

[7] Haddadin S, Albu-Schaffer A, De Luca A, Hirzinger G. Evaluation of Collision Detection and Reaction for a Human-Friendly Robot on Biological Tissues. IARP International Workshop on Technical challenges and for dependable robots in Human environments 2008;.

[8] (DLR) GAC. Safe Human-Robot Interaction;Available from: http:// www. youtube. com/ watch?v= dnUwqngH0bM.

[9] Sander CS, Knutti JW, Meindl JD. A monolithic capacitive pressure sensor with pulse-period output. Electron Devices, IEEE Transactions on. 1980 May;27(5):927–930.



(a) Before impact testing

(b) After impact testing

(c) The destroyed sensor

FIGURE 7. Impact testing results of the sensor system.

[10] Someya STISKYKH T, Sakurai T. A large-area, flexible pressure sensor matrix with organic field-effect transistors for artificial skin applications. PNAS. 2004;101(27):9966–9970.

[11] Abeysinghe DC, Dasgupta S, Boyd JT, Jackson HE. A novel MEMS pressure sensor fabricated on an optical fiber. Photonics Technology Letters, IEEE. 2001 Sept;13(9):993–995.

[12] Palasagaram JN, Ramadoss R. MEMS-Capacitive Pressure Sensor Fabricated Using Printed-Circuit-Processing Techniques. Sensors Journal, IEEE. 2006 Dec;6(6):1374–1375.

[13] Krondorfer RH, Kim YK. Packaging Effect on MEMS Pressure Sensor Performance. Components and Packaging Technologies, IEEE Transactions on. 2007 June;30(2):285–293.

[14] Nakamura K ITYT, K O. MEMS Pressure Sensor. US Patent 8516905 B2;.

[15] Daly MM, Knorr D. Chitosan-Alginate Complex Coacervate Capsules: Effects of Calcium Chloride, Plasticizers, and Polyelectrolytes on Mechanical Stability. Biotechnology Progress. 1988;4(2).

[16] Huguet ML, Dellacherie E. Calcium Alginate Beads Coated with Chitosan: Effect of the Structure of Encapsulated Materials on Their Release. Process Biochemistry. 1996;31(8):745–51.

[17] Jussilaa LAPM J, Kulomaki E. Ballistic skin simulant. Forensic Science International. 2005 May;150:63–71.

[18] Brettuns Village Leather M Lewiston;Available from: http://www. brettunsvillage. com/ leather/ sides.htm.

[19] Harvey MJH E N, Butler EGea. Mechanism of wounding. in: J.B. Coates (Ed.), Wound Ballistics. US Army Surgeon General, Washington DC. 1962;p. 143–235.

[20] Bir C. The evaluation of blunt ballistic impacts of the thorax. Wayne State University. Detroit, Michigan,USA; 2000.

[21] Viano DC, King AI. Biomechanics of chest and abdomen impact. CRC Press, Boca Raton; 2008.

[22] Jussilaa J. Preparing ballistic gelatin-review and proposal for a standard method. Forensic Sci Int. 2004 May;141:91–98.

[23] Gelatin Innovations I Schiller Park;Available from: http://www.gelatininnovations.com/.

[24] Robots and Robotic Devices-Industrial Safety Requirements-Collaborative Industrial Robots, ISO TC 184/SC 2 N/PDTS 15066: Under preparation; 2015.

A Hybrid Method for Manufacturing Text Mining Based on Document Clustering and Topic Modeling Techniques

Peyman Yazdizadeh Shotorbani[1], Farhad Ameri [1]

Boonserm Kulvatunyou [2] , Nenad Ivezic [2]

[1]Engineering Informatics Group, Texas State University, San Marcos, U.S.A
{p_y9, ameri }@txstate.edu
[2]Engineering Laboratory, National Institute of Standards and Technology (NIST)
Gaithersburg, U.S.A
{ boonserm.kulvatunyou, nenad.ivezic}@nist.gov

Abstract.
As the volume of online manufacturing information grows steadily, the need for developing dedicated computational tools for information organization and mining becomes more pronounced. This paper proposes a novel approach for facilitating search and organization of textual documents and also extraction of thematic patterns in manufacturing corpora using document clustering and topic modeling techniques. The proposed method adopts K-means and Latent Dirichlet Allocation (LDA) algorithms for document clustering and topic modeling, respectively. Through experimental validation, it is shown that topic modeling, in conjunction with document clustering, facilitates automated annotation and classification of manufacturing webpages as well as extraction of useful patterns, thus improving the intelligence of supplier discovery and knowledge acquisition tools.

Keywords: text mining, topic modeling, document clustering, supplier discovery, manufacturing service, knowledge acquisition

1 Introduction

Manufacturing companies are increasingly enhancing their web presence in order to improve their visibility in the global market and generate high quality leads. Besides using conventional webpages, manufacturing companies publish online white papers, case studies, newsletters, blogs, info-graphics, and webinars to advertise their capabilities and expertise. This has resulted in rapid growth in the volume of online manufacturing infor-

Shotorbani, Peyman; Ameri, Farhad; Kulvatunyou, Boonserm; Ivezic, Nenad.
"A Hybrid Method for Manufacturing Text Mining Based on Document Clustering and Topic Modeling Techniques."
Paper presented at the APMS International Conference, Advances in Production Management Systems, Iguassu Falls, Brazil, Sep 3-Sep 7, 2016.

mation in an unprecedented rate. The online manufacturing information is typically presented in an unstructured format using natural language text.

The growth in the size and variety of unstructured information poses both challenges and opportunities. The challenge is related to efficient information search and retrieval when dealing with a large volume of heterogeneous and unstructured information. Traditional search methods, such as keyword search, with their limited semantic capabilities, can no longer meet the information retrieval and organization needs of the cyber manufacturing era. More advanced computational tools and techniques are needed that can facilitate search, organization, and summarization of large bodies of text more effectively. At the same time, the unstructured text available on the Internet contains valuable information that can be extracted and transformed into business intelligence to support knowledge-based systems.

In this paper, a hybrid *text mining* technique is proposed for processing and categorizing plain-language manufacturing narratives and extracting useful patterns and unseen connections from them. Text mining is the process of deriving new, previously unknown, information from textual resources [5]. There exist multiple text mining techniques, such as summarization, classification, clustering, topic modeling, and association rule mining that can be applied to the manufacturing documents. Text mining techniques are either supervised or unsupervised. In supervised (also known as predictive) techniques, fully labeled data is used for training machine learning algorithms, whereas in unsupervised (also known as descriptive) techniques, no training dataset is required. Supplier classification using supervised text mining technique was previously proposed and implemented [1].

In this research, two unsupervised text mining techniques, namely, clustering based on k-means algorithm and topic modeling based on LDA algorithm, are adopted. Clustering is the process of grouping documents into clusters based on their content similarity, while topic modeling is a method for finding recurring patterns of co-occurring words in large bodies of texts [7]. Clustering and toping modeling can be regarded as complementary techniques since the unlabeled clusters, as the output of clustering process, can be characterized and described by their core theme using topic modeling technique. The *primary objective* of this research is to use document clustering to build clusters of manufacturing suppliers and to use topic modeling to identify the core concepts that form the underlying theme of each cluster. Organization of manufacturing capability narratives into various clusters with known properties will improve the efficiency of the supplier discovery process. Furthermore, extraction of hidden patterns from the capability narratives could lead to generation of useful information and insights about new trends and developments in manufacturing technology.

This paper is organized as follows. The next section discusses the relevant literature in text analytics. The proposed hybrid method is presented in Section 3. This section also provides information about a proof-of-concept experimentation and validation. The paper ends with concluding remarks.

2 Background and Related Works

Text mining has already been applied in areas ranging from pharmaceutical drug discovery to spam filtering and summarizing and monitoring customer reviews [9]. In the manufacturing domain, however, it is a relatively new undertaking.

Kung et. al [2] used text classification techniques for identifying quality-related problems in semiconductor manufacturing based on the unstructured data available in hold records. Dong and Liu [3] proposed a tool for manufacturing website classification in based on determined genres for the websites [3]. Their proposed website classifier works based on a hybrid Support Vector Machine (SVM) algorithm. However, SVM is a supervised technique that requires high quality training data. Therefore, in absence of well-prepared training data, the proposed approach will not yield the expected outcome. To address this issue, researchers have adopted unsupervised approaches that eliminated the need for preparation of pre-labeled data. Topic modeling [4] and Clustering [5] are two prominent unsupervised methods for text classification and mining. While Clustering is a long existing technique, topic modeling is considered to be a relatively new method. Topic modeling techniques are used to discover the underlying patterns of textual data. Probabilistic Latent Semantic Analysis (PLSA) is one of the first topic modeling techniques introduced by Hofmann [6]. PLSA is a statistical technique that discovers the underlying semantic structure of data [7]. PLSA assumes a document is a combination of various topics. Therefore, by having a small set of latent topics or variables, the model can generate the related words of particular topics in a document. One successful application of PLSA is in the bioinformatics context where it is being applied for prediction of Gene Ontology annotations [8]. However, PLSA can suffer from over-fitting problems [9]. Latent Dirichlet Allocation (LDA) [10] extends the PLSA generative model. In LDA method, every document is seen as a mixture of different topics. This is similar to the PLSA, except that topic distribution in LDA has a Dirichlet prior which results in having more practical mixtures of topics in a document. LDA, as a method for topic modeling, has been used in different applications. For instance, [11] discusses a LDA-based topic modeling technique that automatically finds the thematic patterns on Reuters dataset. The main distinctive feature of their proposed method is that it incrementally builds and updates a model of emerging topics from text streams as opposed to static text corpora. Some researchers have applied LDA method to public sentiments and opinion mining in product reviews [12, 13]. Application of LDA-based topic modeling for exploring offline historical corpora is discussed in [14, 15].

Most of the existing methods use either clustering or topic modeling techniques to help users categorize existing data and infer new information from unstructured data. This paper proposes a hybrid model based on clustering and topic modeling methods to facilitate online search and organization of manufacturing capability narratives and also extraction of thematic patterns in manufacturing corpora.

3 Proposed Methodology for Text Mining

The standard method for web-based information search and retrieval is the keyword-based method. For example, in a supplier search scenario, a customer from the medical industry who is looking for precision machining services can simply use *precision machining* and *medical equipment* as the search keywords in a generic search engine. Nevertheless, the sheer size of the returned set would undermine the usefulness of the search result. One way to make the results more useful is to present them to the user as chunks or clusters of similar documents and then characterize each cluster using a set of *features* or *themes*. In the precision machining example, a cluster characterized by features such as *precision machining*, *medical industry*, *inspection*, and *assembly* would be of interest for the user if inspection and assembly were the secondary services that the user is looking for. This work proposes a hybrid text mining technique, which facilitates automatic clustering and characterization of the documents available in a large manufacturing corpus. The overall structure of the proposed approach is demonstrated in Fig. 1. As can be seen in this figure, the proposed approach is composed of four major steps as described below.

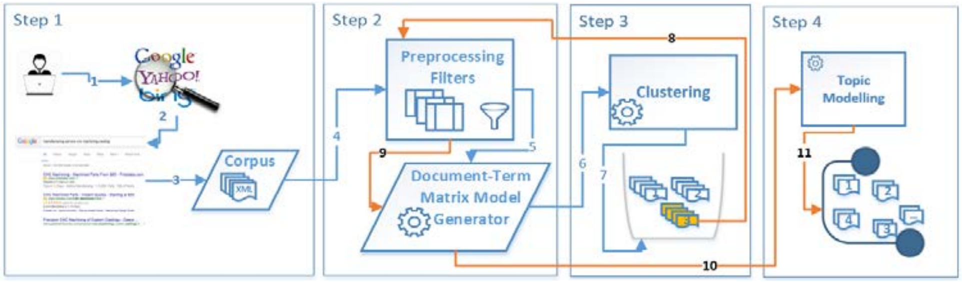


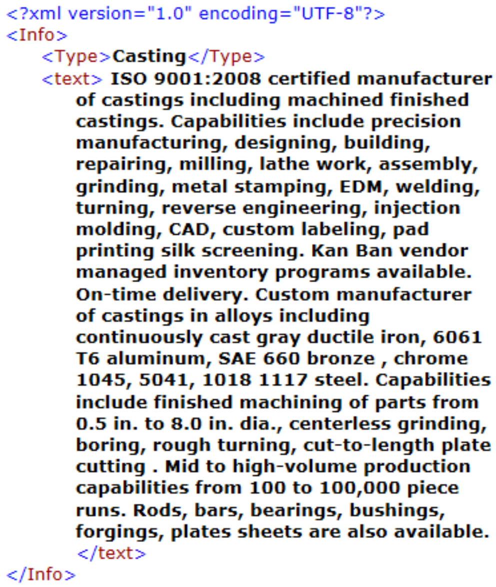
Fig. 1: The Proposed Hybrid Classifier

3.1 Step 1: Building the Corpus

The first step is to create a corpus of manufacturing documents to be used as the test data. The scope of this work was limited to the suppliers of CNC machining and metal casting services. Therefore, to collect relevant websites, a generic web search based on a few keywords such as *machining service*, *contract manufacturing*, casting *service*, *milling*, *turning*, and *sand casting* were used. This keyword-based search is intended to return a set of webpages related to providers of contract manufacturing services. The keywords are selected subjectively based on the requirements of the search scenario and no particular protocol or guideline is used for keyword selection in this work. Each document (i.e., webpages) in the returned set was converted into a text-only document with the XML format. The XML format, due to its generality and simplicity, can be used across different platforms and applications. Fig. 2 illustrates an example of a website that is converted to

Shotorbani, Peyman; Ameri, Farhad; Kulvatunyou, Boonserm; Ivezic, Nenad.
"A Hybrid Method for Manufacturing Text Mining Based on Document Clustering and Topic Modeling Techniques."
Paper presented at the APMS International Conference, Advances in Production Management Systems, Iguassu Falls, Brazil, Sep 3-Sep 7, 2016.

the XML format with only two tags, namely, *type* and *text*. A corpus containing 100 XML documents with13544 terms was created for experimental validation of the proposed approach.



```
<?xml version="1.0" encoding="UTF-8"?>
<Info>
    <Type>Casting</Type>
    <text> ISO 9001:2008 certified manufacturer
        of castings including machined finished
        castings. Capabilities include precision
        manufacturing, designing, building,
        repairing, milling, lathe work, assembly,
        grinding, metal stamping, EDM, welding,
        turning, reverse engineering, injection
        molding, CAD, custom labeling, pad
        printing silk screening. Kan Ban vendor
        managed inventory programs available.
        On-time delivery. Custom manufacturer
        of castings in alloys including
        continuously cast gray ductile iron, 6061
        T6 aluminum, SAE 660 bronze , chrome
        1045, 5041, 1018 1117 steel. Capabilities
        include finished machining of parts from
        0.5 in. to 8.0 in. dia., centerless grinding,
        boring, rough turning, cut-to-length plate
        cutting . Mid to high-volume production
        capabilities from 100 to 100,000 piece
        runs. Rods, bars, bearings, bushings,
        forgings, plates sheets are also available.
        </text>
</Info>
```

Fig. 2: XML-based representation of a document in the corpus

3.2 Step 2: Customized preprocessing of the corpus

Corpus documents need to be noise-free before they can be analyzed and mined efficiently. Corpus preprocessing entails removing the redundant and less informative terms in order to create a clean corpus. The first preprocessing step is to remove numbers, punctuations, and symbols. The next step is to remove the stop words that do not contain significant manufacturing information. The words such as "quote", "inquire", "call", "type", "request", "contact", and "address" that frequently appear in manufacturing websites, but has marginal information about the manufacturing capability, belong to this category. After the removal of numbers, punctuations, symbols, and stop words, the number of words in the corpus is reduced to 10357. Word stemming is the next step in preprocessing which deals with reducing the derived words into their word stem. For example, terms such as "casted" and "casting" are stemmed to "cast". This step is necessary for reducing the dimensionality of data and improving the computational efficiency of the text analytics algorithms. Stemming reduces the number of words to 7470.

The last preprocessing step is to generate the Document-Term Matrix (DTM) for the manufacturing corpus. DTM is a matrix containing the frequency of the terms in the manufacturing documents. In the DTM, documents are denoted by rows and the terms are represented by columns. If a term is repeated *n* times in a specific document, the value of its corresponding cell in the matrix is *n*. The DTM represents the vector model of the corpus and is used as the input to the next step, document clustering.

3.3 Step 3: Document Clustering

This step involves creating groups of similar documents in the corpus. In this work, a *K-Means clustering* algorithm is implemented which automatically clusters the documents of the corpus such that documents in a cluster are more similar to each other than the documents in other clusters. In K-Means clustering technique, the user needs to specify the number of clusters (*K*) in advance [16]. Then the algorithm defines K centroids, one for each cluster. The next step is to assign each document to the nearest centroid. The distance from a document to the centroids of the clusters is calculated based on the projection of multidimensional DTM on Euclidean planes. The objective function of the k-means algorithms is to minimize the sum of square of distances from the data points (i.e., documents) to the clusters. Therefore, multiple iterations are required until the convergence condition is met. The main steps of the clustering algorithm are listed below:

1. Randomly distribute the documents among the K predefined clusters.
2. Calculate the position of the centroid of each cluster.
3. Calculate the distance between each document and each centroid
4. Assign each document to the closets centroid.
5. Iterate over steps 1 to 4 until each document is assigned to at least one cluster, no document is relocated to a new cluster, and the convergence condition is met.

To estimate the proper number of clusters in the dataset, the Sum of Squared Error (SSE) method is used in this work. SSE refers to the sum of the squared distance between each document of a cluster and the centroid of the cluster. The corpus holds 100 documents. Therefore, the value of K ranges from 2 to 99. The challenge is to select the proper number of clusters through investigating the SSE corresponding to each cluster. Generally, as it is depicted in Figure 3, when the number of clusters increases from 2 to 99, the SSE decreases since the clusters become smaller in size.

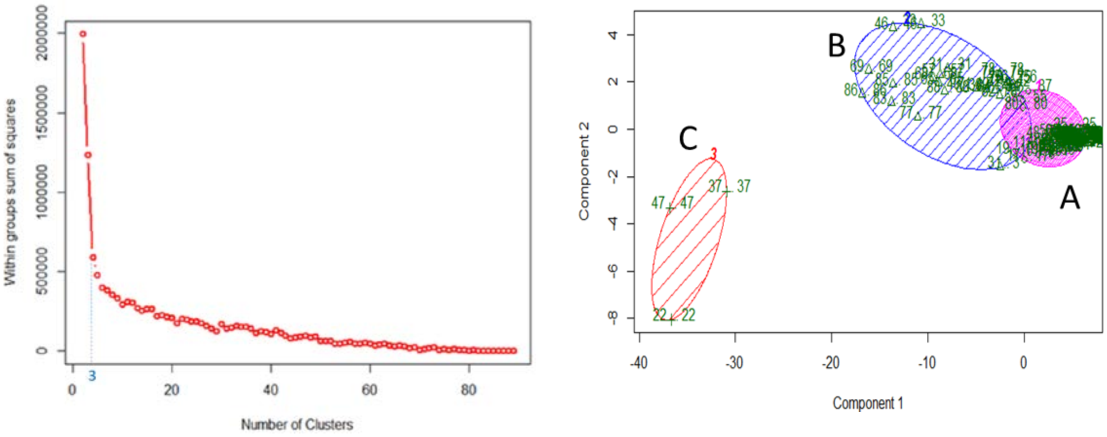


Fig. 3: SSE curve for different values of k

Fig. 4: Result of clustering

Based on the SSE plot, the suggested number of clusters is determined by the point where the sharp drop in SSE ends [16]. This points is referred to as the *elbow point*. As can be seen in Fig. 4, the elbow point occurs where the number of clusters is equal to 3. Therefore, three clusters were generated for this particular dataset. These three clusters with their assigned manufacturing documents are illustrated in Fig.4.

The plot of clustering result, shown in Fig.4, is obtained based on a dimension reduction technique called Principle Component Analysis (PCA). The proposed clustering algorithm is based on the number of words in the corpus (7470 words or dimensions) which makes it impossible to visualize the documents of the clusters. To overcome this problem, PCA is used to enable the projection all data points (i.e., documents) on a 2D plane.

As it can be seen in the plot, the two upper right clusters (clusters A and B) have partial overlap, while the third cluster (Cluster C) in the lower left corner is clearly distinct from the other two. After inspecting the clusters, it was revealed that the members of the overlapped clusters (A and B) were the websites of contract manufacturers who offer machining and casting services. The distinctive feature of the overlapping clusters is the depth of information provided by the member websites. The websites in cluster A contain general and high-level information about the type of process and services the suppliers offer while the websites in cluster B provide more detailed information about the type of processes, sub-processes, secondary services, and materials offered by the company. Cluster C mainly contained trade websites, blogs, or technical white papers. This experiment demonstrated that the clustering algorithm can successfully build meaningful clusters based on the type and nature of documents and also the level of detail incorporated in them. However, the clustering algorithm did not make a distinction between machining and casting websites. Also, it is not possible to learn about the characteristics of each cluster without exploring each cluster and investigating its contents. To further analyze and explore each cluster automatically, topic modeling technique is used in the next step. Cluster B, which contains 50 documents, is selected as the input to the topic modeling process.

3.4 Step 4: Topic Modeling

Document clustering results in partitioning a heterogeneous dataset into multiple clusters with more similar members. However, it doesn't provide any description or characterization for the generated clusters. Topic Modeling is a text mining technique for analyzing large volumes of unlabeled text. Latent Dirichlet Allocation (LDA) is used as the underlying algorithm for topic modeling. LDA technique can be used for automatically discovering abstract topics in a group of unlabeled documents. A *topic* is a recurring pattern of words that frequently appear together. For example, in a collection of documents that are related to banking, the terms such as *interest*, *credit*, *saving*, *checking*, *statement*, and *APR* define a topic as they co-occur frequently in the documents. LDA technique assumes that each document in the dataset is randomly composed of a combination of all available topics with different probabilities for each. The basic steps of the LDA technique are listed below. The reader is referred to [4] for more detailed discussion of the LDA technique:

1. For each document *d*, randomly allocate each word in the document to one of the *t* topics. This random allocation provides topic representations of all the documents and also distributions of words of all the topics.
2. For each document *d*, calculate two values.
    a. p (topic t | document d), which is the proportion of words in document *d* which are currently assigned to topic t
    b. p (word w | topic t), which is the proportion of allocations to topic *t* over all available documents that are using word *w*.
3. Reassign the word *w* to a new topic.
4. Repeat the steps 1 through 3 until a steady state is achieved where the word-to-topic assignments sound meaningful.

As the last stage of the experiment, the application is run to find a predetermined number of topics in the dataset. The number of topics depends on the diversity of the documents in the dataset. More diverse documents discuss more topics, whereas more focused documents are centered around only a few themes. In this experiment, the desirable number of topics was set to *four* after studying the documents and their themes. Table 1 shows these four topics and their 10 most frequent words.

Table 1: Top 10 stemmed terms in Topic 1 through Topic 4

	Topic 1	Topic 2	Topic 3	Topic 4
1	turn	cast	cnc	machine
2	service	die	turn	custom
3	steel	mold	part	process
4	industry	aluminum	tool	product
5	component	sand	equip	quality
6	alloy	housing	mill	manufacture
7	format	iron	material	high
8	stainless	rang	product	engine
9	standard	test	chuck	grind
10	aerospace	system	precision	provide

From Table 1, it can be inferred that Topic 2 is mainly about *casting processes* while Topic 3 corresponds to the *turning and milling processes*. However, as mentioned earlier, each document can address more than one topic. The LDA addresses this issue by returning topic probabilities associated with each document. Table 2 lists these probabilities for five example documents in the dataset.

Table 2: Documents and their topic probabilities

Document	Topic 1	Topic 2	Topic 3	Topic 4
1.xml	0.091	**0.166**	**0.554**	**0.187**
2.xml	**0.609**	0.053	0.223	0.113
4.xml	0.149	**0.659**	0.085	0.105
5.xml	**0.215**	**0.203**	**0.226**	**0.354**

From Table 2, it can be concluded that the first document belongs to topic 3 which is mainly about CNC machining services. Also, the calculated probabilities suggest that the fourth document belongs to topic 2, which corresponds to the casting process and services. Furthermore, document 5 equally discusses topics 1 through 5 which implies that the supplier pertaining to this document is not specialized in only one manufacturing process. The performance of the proposed technique can be improved in time by adding more terms to the list of stop words that will be filtered out at the preprocessing stage. For example, the terms *component* and *format* under topic 1 are not as informative as the other terms in the group and can be eliminated from the vector model.

4 Conclusions

This paper presents a hybrid text mining method based on document clustering and topic modeling techniques. The objective of the proposed method is to build clusters of manufacturing websites and discover the hidden patterns and themes in the identified clusters. Furthermore, it harvests the key manufacturing concepts that can be imported into manufacturing thesauri and ontologies. Given the unsupervised nature of the algorithms used in this work, there is no need to prepare training data. This significantly reduces the initial setup cost and time. The results provided in this paper are only based on a single run of the mining process. The performance of the proposed method can be further improved through multiple iterations and subsequent elimination of less informative words under each topic. When highly informative terms are clustered together under a topic, the likelihood of discovering useful patterns in data increases. The corpus used in this proof-of-concept implementation contains only 100 documents. To reap the true benefits of text mining in manufacturing, the size of the corpus has to be significantly larger.

There are multiple areas that can be further explored in the future. One future task is to evaluate the performance of different topic modeling algorithms that can be used in the proposed framework. In the current implementation, the number of topics is determined upfront by the user, but there is a need for calculating the optimum number of topics in the corpus automatically.

Acknowledgement: The work described in this paper was funded in part by NIST cooperative agreement with Texas State University No. 70NANB14H255.

References

[1] Yazdizadeh, P., and Ameri, F.: A Text Mining Technique for Manufacturing Supplier Classification, ASME IDETC 2015, 35th Computers and Information in Engineering (CIE) Conference (2015)

[2] Liu, Y., Kung, J., J, L., and Y.B, H.: Using text mining to handle unstructured data in semiconductor manufacturing, Joint e-Manufacturing and Design Collaboration Symposium (eMDC), International Symposium on Semiconductor Manufacturing (ISSM), (IEEE, Piscataway, NJ, USA), 1-3 (2015)

[3] Dong, B., and Liu, H.: Enterprise Website Topic Modeling and Web Resource Searc", Sixth International Conference on Intelligent Systems Design and Applications (2006).

[4] Blei,D.: Probabilistic topic models , Communications of the ACM, 55(4) (2012)

[5] Manning, C., Raghavan, P., and Schütze, H.: Introduction to information retrieval, Cambridge University Press, New York (2008).

[6] Hofmann, T.: Probabilistic Latent Semantic Indexing, Proceedings of the 15th Conference on Uncertainty in Artificial Intelligence (1999)

[7] Steyvers, M. and Griffiths, T. L.: Probabilistic Topic Models," In T. Landauer, D McNamara, S Dennis, and W. Kintsch (ed), Latent Semantic Analysis: A Road to Meaning, Laurence Erlbaum (2005)

[8] Masseroli, M., Chicco, D., and Pinoli, P.: Probabilistic Latent Semantic Analysis for prediction of Gene Ontology annotations, The 2012 International Joint Conference on Neural Networks (2012).

[9] Alghamdi, R., and Alfalqi, K.: A Survey of Topic Modeling in Text Mining, International Journal of Advanced Computer Science and Applications, 6(1) (2015).

[10] Blei, D. M., Ng, A. Y., & Jordan, M. I.: Latent Dirichlet allocation. Journal of Machine Learning Research, 3, 993–1022 (2003)

[11] AlSumait, L., Barbará, D., and Domeniconi, C.: On-line LDA: Adaptive Topic

Models for Mining Text Streams with Applications to Topic Detection and Tracking, 2008 Eighth IEEE International Conference on Data Mining (2008).

[12] Shulong, T., Yang L., Huan, S., Ziyu, G., Xifeng, Y., Jiajun, B., Chun, C., and Xiaofei, H.: Interpreting the Public Sentiment Variations on Twitter", IEEE Trans. Knowl. Data Eng., 26(5), 1158-1170 (2014)

[13] Zhongwu, Z., Bing, L., Hua, X., Peifa, J..: Constrained LDA for grouping product features in opinion mining. In Proceedings of PAKDD, pages 448–459 (2001)

[14] Hu, Y., Boyd-Graber, J., Satinoff, B., and Smith, A.: Interactive topic modeling, Mach Learn, 95(3), pp. 423-469 (2013)

[15] T.I. Yang, A.J. Torget, and R. Mihalcea, Topic modeling on historical newspapers, In Proceedings of the 5th ACL-HLT Workshop on Language Technology for Cultural Heritage, Social Sciences, and Humanities, pages 96–104 (2011).

[16] Kodinariya, T.M., Makwana, P.R.: Review on determining number of Cluster in K-Means Clustering". International Journal of Advance Research in Computer Science and Management Studies 1(6), 90-95 (2013)

Towards a Reconfigurable Distributed Testbed to Enable Advanced Research and Development of Timing and Synchronization in Cyber-Physical Systems

Hugo A. Andrade ¶, Patricia Derler ¶, John C. Eidson ‖, Ya-Shian Li-Baboud‡,
Aviral Shrivastava*, Kevin Stanton†, Marc Weiss §
¶ National Instruments, Berkeley, CA
‖ University of California, Berkeley
‡ NIST Software and Systems Division, Gaithersburg, MD
* Arizona State University
† Intel Corporation, Hillsboro, OR
§ NIST Time and Frequency Division, Boulder, CO

***Abstract*—Timing and synchronization play a key role in cyber-physical systems (CPS). Precise timing, as often required in safety-critical CPS, depends on hardware support for enforcement of periodic measure, compute, and actuate cycles. For general CPS, designers use a combination of application specific integrated circuits (ASICs) or field programmable gate arrays (FPGAs) and conventional microprocessors. Microprocessors as well as commonly used computer languages and operating systems are essentially devoid of any explicit support for precise timing and synchronization. Modern computer science and microprocessor design has effectively removed time from the abstractions used by designers with the result that time is regarded as a performance metric rather than a correctness specification or criterion.**

There are interesting proposals and avenues of research to correct this situation, but the barrier is quite high for conducting proof of concept studies or collaborative research and development. This paper proposes a conceptual design and use model for a reconfigurable testbed designed specifically to support exploratory research, proof of concept, and collaborative work to introduce explicit support for time and synchronization in microprocessors, reconfigurable fabrics, language and design system architecture for time-sensitive CPS.

Reconfigurable computing is used throughout the system in several roles: as part of the prototyping platform infrastructure, the measurement and control system, and the application system under test.

***Index Terms*—Cyber-Physical Systems, Timing and Synchronization, Reconfigurable computing, Testbed, Correct-by-construction**

I. Motivation

Timing and synchronization play a key role in cyber-physical systems (CPS). The typical CPS implements a measure, compute, and actuate cycle. To ensure stability of the resulting control loop, a fundamental requirement is to control the loop time. As CPS become more complex with multiple sensors driving the control function and possibly with multiple actuators involved, the timing becomes even more critical in ensuring precise coordination and control. For example, each application will specify the temporal relationships between the sensor data, usually requiring simultaneous sampling within some tolerance. Likewise, any resulting actuation will have similar temporal constraints.

Traditionally, sensors and actuators communicate directly with the CPS controller via analog lines, point-to-point digital links, or via a specialized data bus such as controller area network (CAN) or highway addressable remote transducer (HART) protocols. In modern designs, the spatial extent or the need for greater bandwidth has resulted in CPS with multiple controllers, involving networks for communication. The control of timing in such systems is much more difficult than in the earlier, compact systems.

For safety-critical systems, time-triggered techniques are often used and depend on hardware support for enforcement of periodic measure, compute, and actuate cycles. Time-triggered architectures are relatively inflexible and do not scale well. In addition the model is a poor match for systems with asynchronous sporadic inputs. For general CPS, designers must use a combination of ASICs or FPGAs and conventional microprocessors.

Unfortunately, modern computer science and microprocessor design have effectively removed explicit time from microprocessor hardware, operating systems and languages with the result that time is essentially a performance metric rather than a correctness specification or criterion [1]. Without the semantics and standard interfaces to specify timing requirements, it becomes costly and difficult to build a CPS with robust timing leading to a methodology where system timeliness issues are corrected through test and adjustment. This methodology results in customized, application specific designs which are expensive to maintain and commission. Furthermore, system components are less likely to be interoperable and adding or swapping components can result in

Shrivastava, Aviral; Eidson, J; Weiss, Marc; Li-Baboud, YaShian; Andrade, Hugo; Derler, Patricia; Stanton, Kevin.
"Towards a Reconfigurable Distributed Testbed to Enable Advanced Research and Development of Timing and Synchronization in Cyber-Physical Systems."
Paper presented at the 2015 International Conference on Reconfigurable Computing and FPGAs, Mayan Riviera, Mexico, Dec 7-Dec 9, 2015.

costly re-validation of timing requirements. Users of major or critical CPS systems often purchase a lifetime supply of all components since the replacement of a hardware component, e.g. a faster microprocessor, or a change in code or firmware typically results in expensive re-qualification of the system.

In a time-triggered architecture, it is necessary to ensure that the computations can be completed in the allotted time. In a CPS utilizing general purpose hardware and software, the task of ensuring correct timing is even more difficult. What is clearly needed is a systematic design methodology where the designer can explicitly specify system timing and given a target computer, software, and network environment, be able to determine whether the proposed design can actually be executed in this environment with the proposed timing. Finally if the answer is yes, then the designer should be able to compile the design into an executable form with the assurance that during execution the system timing will agree to the designed timing within specified error bounds. This is simply not possible today using general purpose software development tools and hardware platforms.

There are interesting proposals and avenues of research to correct this situation, but the barrier is quite high for conducting proof of concept studies or to conduct collaborative research and development on this subject.

In this paper, we describe our vision for a testbed and usage model designed specifically to support research, proof of concept, and collaborative work to introduce explicit support for time in microprocessor, reconfigurable fabrics, language and design system architecture for time-sensitive CPS.

The ultimate outcome of the research enabled by the proposed testbed should be the development of modular, interoperable system components including novel microprocessor architectures, software design, communication interfaces, compilers and semantics where timing correctness can be explicitly described and verified. Explicit time specifications can be enunciated, incorporated into application and software/firmware design and executed in such a way that the timing in the executing system matches the time specifications of the designer to within the accuracy of the CPS real-time clock. In other words, the ultimate goal is to enable *correct-by-construction* CPS system timing.

II. Testbed research challenge areas

One of the primary impediment to a designer's ability to have correct-by-construction timing is the availability of explicit support for time in the code stack from microprocessor to hardware, e.g., to support design requirements such as "raise on pin 3, a signal x microseconds following the time a signal was raised on pin 2 to within the precision of the local clock where x is a value determined at run time by system state". Timing specific instructions cannot be specified such that it would be reliably executed today except by custom design in ASICs or FPGAs. If explicit time was appropriately supported, then it would be possible to design true, portable real-time operating systems (OS), programming languages would emerge to build on this capability, and time-sensitive application and communication design practices would follow.

One of the key research challenges is enabling bounded timing support in the code stack. Of course there have been prior efforts in this direction [2]. Another example is the Programming Temporally Integrated Distributed Embedded Systems (PTIDES) model developed at the University of California Berkeley [3]. More research challenges and potential solutions have also been discussed in the National Institute of Standards and Technology (NIST) Cyber-Physical Systems Public Working Group [4]. Stemming from the challenge of enabling hardware agnostic timing support in the code stack is the ability to define common semantics and interfaces to enable correct-by-construction on a variety of microprocessors. Another research challenge is the ability to measure and verify that the system can achieve worst-case bounded timing or be able to handle graceful degradation if timing requirements are not achieved.

There are of course other issues such as providing synchronized clocks in each node and ensuring that network communications realize timing specifications. However the state of the art in clock synchronization is quite good using available technologies such as Global Navigation Satellite Systems (GNSS), Network Time Protocol (NTP) [5], IEEE 1588 Precision Time Protocol [6], or Conseil Europen pour la Recherche Nuclaire's (CERN) White Rabbit [7][8]. The situation with networks is less satisfactory but there is a concerted ongoing effort in the IEEE 802 community to enable time-sensitive networking (TSN) [9].

We envision a distributed testbed bringing together a community of multi-disciplinary experts to enable exploration of time aware interfaces, methodologies, and measurement capabilities to the simple CPS architecture diagrammed in Figure 1. Illustrated are four CPS nodes communicating via a fabric and with each node interacting with the external physical world to be measured and/or controlled.

As illustrated, each node consists of a system stack with custom hardware at the bottom, interacting with the external physical world and the communication fabric. This layer is typically a combination of an FPGA, digital to analog converters (DACs), analog to digital converters (ADCs), communication physical layer (PHYs), input/output (I/O) etc., with standard computer interfaces to the operating system of the microprocessor. The designer creates code running on the microprocessor and a closely connected or integrated reconfigurable fabric, which in conjunction with the underlying hardware, realizes the functional and timing specifications of the CPS.

The following sections describe a conceptual design and use model for a testbed designed specifically to support research, proof of concept, and collaborative work to introduce explicit support for time in microprocessor, reconfigurable fabrics, language and design system architecture for time-sensitive CPS. Because the testbed includes a physical monitoring and control scenario, it will be possible to quantitatively compare different approaches by measuring the timing performance of

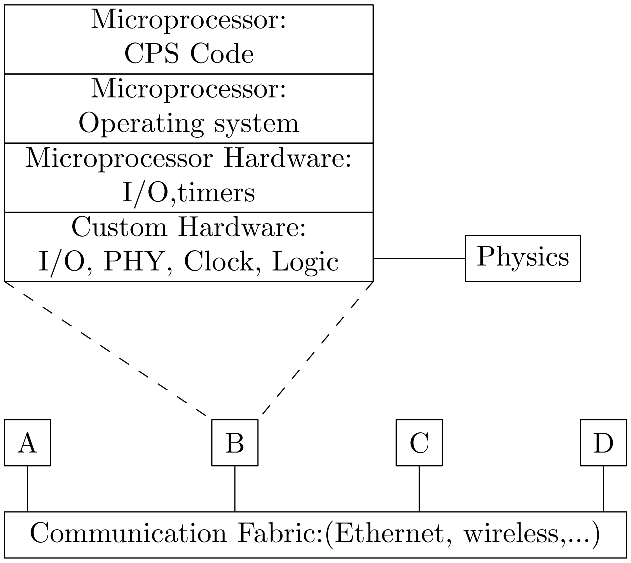


Fig. 1. Simple CPS

two or more proposed designs. One of the objectives of the testbed architecture is to support the exploration of application designs and practices in explicit timing support in hardware, operating system and code design stack of underlying real-time applications. For distributed systems, the proposed testbed could be expanded to enable research on time-sensitive network components and practices.

III. The testbed architecture

The proposed testbed architecture is illustrated in Figure 2. The key elements are as follows:

- Four CPS nodes described in section III-A. These are connected to a communication fabric and interface to testbed physics.
- Communication fabric: Standard gigabit Ethernet implemented with an IEEE 1588 bridge to enable precise clock synchronization among the distributed nodes. Synchronization is needed to ensure timing requirements can be estimated and measured in a distributed system.
- Physics: A selection of devices to be used in simple CPS applications. See section III-B.
- Physics Monitoring and Control: Instrumentation to monitor, configure and control the experiment physics to provide ground truth timing measurements for comparison with the specifications of the CPS system being tested. See section III-C.
- Testbed Site Computer: The computer has three main functions:
  - Communication Monitor and Device Configuration: This interface monitors traffic on the testbed communication fabric, e.g., with Wireshark. It also interfaces with the Physics Monitoring and Control instrumentation. It provides the interface to the four CPS nodes for downloading node FPGA and software.
  - Local Testbed Management: Manages the operation of the testbed. Included is user session management, loading of default CPS node designs, etc. A repository of testbed site approved introductory code samples similar to “hello world” would be maintained here. The repository of code contributed will enable the community to share code and evolve the algorithms and software implementations to ensure hardware portability and system scalability as each user may apply improve upon the code to fit their use case and system. The repository will also aid in growing the ontology for enabling explicit timing support by exploring frequently used semantics needed to describe the timing requirements. Through exposure to a wide variety of CPS use cases as well as experimental algorithms and methodologies, the distributed testbed will enable the community to ensure semantics for explicit timing support are adequately captured and provide the flexibility needed to meet a wide range of CPS timing requirements. Flexibility in application requirements and hardware relies on a high quality, stable and complete ontology to describe the features that are pertinent to reliable system timing. See section III-D.
  - Interface to Remote Users: Provides an interface to remote user sites to permit download of CPS node design, monitoring of the network, CPS node performance, and physics monitoring and control. It provides security and login functions.
- Internet: The public Internet is used for communications between remote user sites and testbed sites.
- User Site Computer: The user site computer has the following functions:
  - Interface to Remote Testbed: Provides an interface to remote user sites to permit download of CPS node design, network monitoring, CPS node performance, and physics monitoring and control. It also provides security and login functions.
  - User Interface, Design and Configuration Tools: The interface enables exploration of explicit timing support methodologies, such as PTIDES, to allow a remote user to generate FPGA design, to program and compile software for the microprocessor, to download FPGA designs and code executables, and to monitor and configure the CPS. FPGA design interfaces and code compilers could execute on the client side or done remotely on tools executing at the remote testbed site. The tools and the testbed would enable experimenting with different:
    - ∗ designs for hardware support of explicit time,
    - ∗ designs for true real-time operating systems,
    - ∗ languages, compilers, and other software development infrastructure

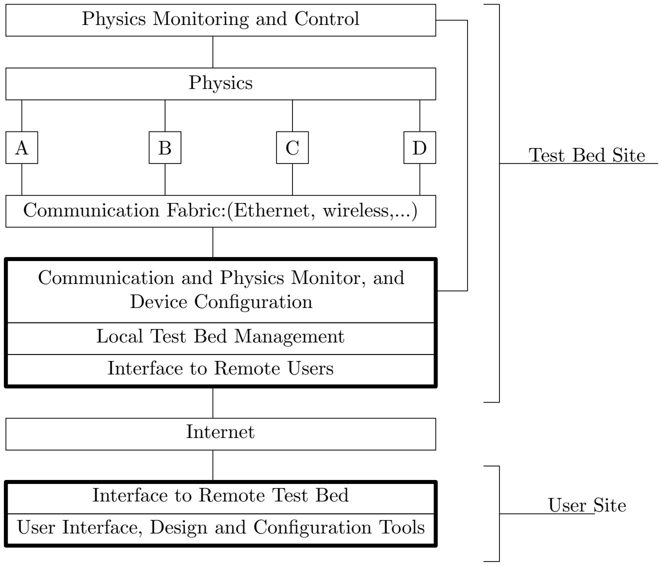

Physics Monitoring and Control
Physics
A
B
C
D
Communication Fabric:(Ethernet, wireless,...)
Communication and Physics Monitor, and Device Configuration
Local Test Bed Management
Interface to Remote Users
Test Bed Site
Internet
Interface to Remote Test Bed
User Interface, Design and Configuration Tools
User Site

Fig. 2. Testbed Architecture

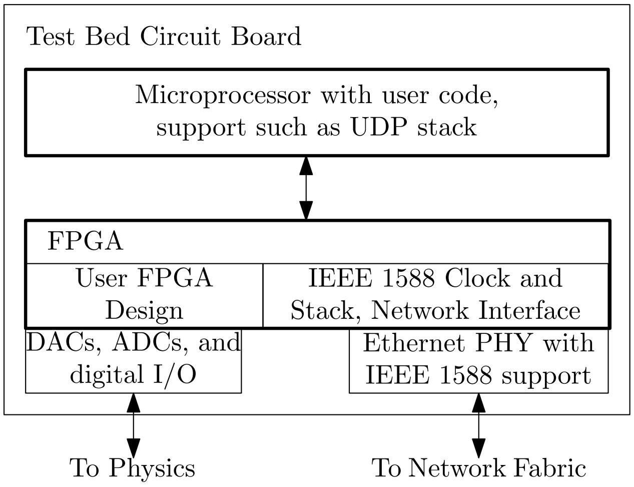

Test Bed Circuit Board
Microprocessor with user code, support such as UDP stack
FPGA
User FPGA Design
IEEE 1588 Clock and Stack, Network Interface
DACs, ADCs, and digital I/O
Ethernet PHY with IEEE 1588 support
To Physics
To Network Fabric

Fig. 3. Testbed Node Architecture

∗ techniques for exploiting explicit time in applications both within a single node and in a distributed CPS system.

A. Testbed CPS Node Architecture

The architecture of each of the four CPS testbed nodes is illustrated in Figure 3 and consists of a circuit board with the following components:

- An FPGA: A fairly large FPGA to give users plenty of room to try out designs. Several options will be supported: the FPGA can have resident microprocessors either for user code or to implement all or part of the network or clock synchronization stacks, or the FPGA will serve as an interface to a separate chip level implementation of the microprocessor design. In any case, the FPGA will contain IEEE 1588 hardware clock to provide synchronized clock service among the peers in the CPS. It also contains any needed network interface. The clock will interface to user FPGA designs and/or to the microprocessor. It should be noted that it is our intent to support new and evolving standards such as the IEEE TSN [9].
- A microprocessor: The specific microprocessor, associated memory and support are to be determined as well as whether a different microprocessor should be on each board to allow investigation/proof that a explicit timing support methodology, such as correct-by-construction, can be invariant to microprocessor speed, cache size, etc. The testbed intends to include a wide range of hardware designs for supporting explicit time. Some of the hardware currently shown in the FPGA block may reside in the microprocessor.
- Ethernet PHY with IEEE 1588 support: These PHYs are readily available and simplify the implementation of the IEEE 1588 stack. The PHY will also provide data connectivity to the gigabit network fabric.
- Physics interface: A selection of DACs, ADCs and digital I/O will be provided. The specifics depend on the details of the experimental physics section of the testbed.

B. Testbed CPS Physics

The testbed physics enables testing of time sensitive designs applied to realistic CPS applications and the comparison of alternative designs. The selection of components should be simple at first but at a minimum should provide devices suitable for analog, digital and frequency dependent applications. Examples might include one or more of the following:

- Two small laboratory bench size motor-generator sets, mock transmission lines, capability to measure waveforms or phase, and capability to connect/disconnect from a load. This could be used to mimic power system applications such as synchronizing two generators prior to connecting to a load.
- A digital pattern generator and capture device to allow testing of stimulus response applications with sporadic or patterned signals.
- Two or more vibration sensors, perhaps mounted on the motor-generators to allow testing of machine condition monitoring style applications where frequency control of ADCs is important.
- The physics could be implemented in a Hardware-in-the-Loop (HIL) simulation manner, in which a powerful computer is running a model of the physics in real-time.

C. Testbed CPS Physics Monitoring

The testbed monitoring capabilities will depend on the specifics of the testbed physics. The monitoring will generate a variety of time series data which could be fused together from local or remote locations. Ideally the physics and monitoring should be designed together and in many cases can be implemented using standard small scale laboratory equipment available from several manufacturers. In some cases this equipment can be synchronized to the IEEE 1588 timescale to simplify comparison of ground truth monitoring with the results obtained from the CPS nodes. In the case where the physics are done via HIL simulation, physics monitoring would be integrated into the model and connected directly to the rest of the system.

D. Testbed Hello World Examples

As with any set of tools, users will experience a learning curve. A proven way to shorten the learning curve is to provide hello world examples that illustrate how to formulate the FPGA and code designs, load them into the testbed and observe the results. The current testbed design is comprised of:

- A simple time-triggered application: The measure, compute, and actuate cycle could be implemented in the FPGA in combination with microprocessor code. This would be suitable for implementing the power generation test example mentioned in section III-B. This technique is discussed in [10].
- A PTIDES-based application: The PTIDES model [3] could be implemented for a simple control or measurement system. The power systems example would be appropriate as would monitoring and response to sporadic signals. Such a test application is described in [11].
- A National Instrument (NI) Reconfigurable I/O (RIO) system, where the application under test could be developed in LabVIEW using both Real-Time and FPGA modules, implemented on a CompactRIO controller, and the physics could either be a physical experiment and NI-PXI equipment would be used as measurement and control, or the Physics could be an HIL simulation implemented in NI PXI equipment using real-time and FPGA RIO hardware and software, and the measurement and control sub-system would be integrated with the physics. [12]

IV. The testbed usage model

Initially we envision separate testbeds at the location of the core group of participants. This will make it easier to converge on a suitable and robust design for the testbed. As the number of users grows we will want to replicate all or part of the testbed in their own facilities. The testbed hardware and software tools would be open source.

- The designs, code and parts lists will be made available to the technical community.
- Once the testbed model is deployed, the idea would be to expand towards a modular, distributed testbed to enable remote access to one or more locations that would be available to researchers and to encourage collaborative efforts. *One of our goals in presenting this paper at this conference is to solicit open feedback and start building a community around this effort.*

Ideally researchers in remote locations could reserve time on a testbed. Remote access to the testbed would provide monitoring of usage, agreement on testbed policy, etc. They would use the provided design tools to implement their designs which would then be loaded onto the testbed. Execution would be monitored by the users to verify performance and correctness of the implementation.

After some experience with the testbed, it might be appropriate to provide additional open source examples. *The repository is critical to publicizing successful developments arising out of the use of the testbed.* What is needed is the ability of interested researchers and potential industrial users to leverage the proposed solutions and to experiment with the code without having to recreate the entire system in their own facility.

Provision would be made for multidisciplinary researchers to collaborate enabling systems, compilers and networking researchers, among others, can evolve their technologies realize correct-by-construction.

Finally it is critical to develop clear, well documented examples and tutorials to encourage and educate system designers and developers. Depending on the selection of the initial example this work should be done by people with experience with the example techniques and applications.

V. Benefits of the testbed

Aside from the principal benefit of enabling individual and collaborative research on explicit time support in the node stack, other possible uses and benefits include:

- Allowing semiconductor manufacturers to explore tradeoffs on the distribution and form of hardware timing support in microprocessor, the development of time-explicit tool chains and the like. This capability should shorten their learning curve, allow beta demonstrations to gather customer feedback and make it much easier for manufactures to confidently incorporate the advances arising out of the use of the testbed.
- Plugfest activity: The testbed should be relatively portable which should enable its use for conducting tests and demonstrating the new technologies. The presence of the testbed should encourage expansion of the ideas explored.
- University teaching projects: Many universities include projects for classes in embedded system design, control and related subjects. A distributed testbed enables students to develop code on a variety of platforms for different CPS scenarios, without having to acquire potentially costly equipment.
- Developing a cadre of researchers, students, and others who are familiar with the developed techniques would be of great benefit to societal innovation. One of the barriers to changing system design and programming methodologies is the lack of an experience base and thorough validation. The emerging cadre of experienced students by learning through community and online examples would facilitate adoption and encourage the idea to proliferate in a variety of domains and platforms.

The testbed concept would be an ideal way for industry to rapidly gain experience and innovate safety-critical systems more rapidly.

- As a way of promoting the principles and technologies for time-explicit design, the testbed would be an ideal demonstration platform easily used by application engineers. Introductory, open-source examples would be a boon to proliferating the understanding, adoption and expansion of the ideas.
- The proposed testbed would also benefit standards development and other industry efforts to enable explicit timing support in dealing with CPS.

  The testbed can be particularly useful in allowing research groups and industry to rapidly evaluate academic work in the area of CPS timing and to promote collaborative development of standard interfaces among consortia, government, and academic researchers. As a result, an important aspect of the testbed is to make the interfaces open, generic and interoperable, so that some other equipment or processor can be used to build the system, and evaluated. Such organizations include The AVNU Alliance, http://avnu.org/, the Industrial Internet Consortium (IIC), http://www.industrialinternetconsortium.org/, and the IEEE 802.1 TSN http://www.ieee802.org/1/pages/tsn.html working group.

VI. Role of reconfigurable computing (RC) and FPGA technology in the testbed

Reconfigurable computing and FPGA technology play a key role in this project. It will be used at least in the following subcomponents:

- *System interface for the testbed nodes.* RC/FPGAs will be used to implement the deterministic networking interface and the logic to interface to microprocessors and I/O.
- *Device under Test.* Since the researchers using this facility are mainly trying to test out new technologies, RC and FPGAs provide a great vehicle to test their designs. A shared or dedicated FPGA can used also be part of the testbed node.
- *Deterministic networking.* As part of the system interface, this component will rely on existing (IEEE 1588) or new (IEEE TSN) standards to provide a global notion of time and deterministic data transfer, respectively. Since these are going to be evolving standards, having the flexibility of the FPGA is very important.
- *Physics modeling.* The testbed user has an option of interfacing to the real physics associated with their system, or to simulate the physics with HIL infrastructure based on high performance instruction processors or RC/FPGAs.
- *Measurement infrastructure.* In order to accurately correlate results of the interaction of a CPS cyber-controller and the plant/physics, the measurement infrastructure would interface to the deterministic network using RC/FPGAs to enable measurement processing in real-time. In addition, the testbed would also support measurement capabilities for explicit timing support. Through experience, the efforts of the testbed can determine the pertinent metrics needed to ensure distributed, deterministic, and interoperable timing support.

VII. Conclusion

We have proposed a conceptual design and use model for a reconfigurable testbed designed specifically to support research, proof of concept, and collaborative work to introduce explicit support for time and synchronization in microprocessors, reconfigurable fabrics, language and design system architecture for time-sensitive CPS. Reconfigurable computing is used throughout the system in several roles: as part of the prototyping platform infrastructure, the measurement and control system, and the application system under test.

Disclaimer: Certain commercial entities, equipment, or materials are identified in this document in order to describe the experimental design or to illustrate concepts. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Official contribution of the National Institute of Standards and Technology; not subject to copyright in the United States.

References

[1] E. A. Lee, "Cyber physical systems: Design challenges," in *International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC),.* Orlando, Florida: IEEE, 2008, pp. 363 – 369. [Online]. Available: http://dx.doi.org/10.1109/ISORC.2008.25

[2] P. Caspi, A. Curic, A. Maignan, C. Sofronis, S. Tripakis, and P. Niebert, "From Simulink to SCADE/Lustre to TTA: a layered approach for distributed embedded applications," in *ACM Sigplan Notices*, vol. 38, no. 7. ACM, 2003, pp. 153–162.

[3] Y. Zhao, "On the design of concurrent, distributed real-time systems," PhD, University of California, Berkeley, 2009.

[4] NIST, "NIST Cyber-Physical Systems Public Working Group," 2014. [Online]. Available: http://www.nist.gov/cps/

[5] D. J. Mills, E. Martin, J. Burbank, and W. Kasch, "Network time protocol version 4: Protocol and algorithms specification," University of Delaware, Tech. Rep. RFC 5905, June 2010. [Online]. Available: http://www.hjp.at/doc/rfc/rfc5905.html

[6] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," *IEEE Std. 1588-2008.*

[7] G. Gaderer, P. Loschmidt, E. G. Cota, J. H. Lewis, J. Serrano, M. Cattin, P. Alvarez, P. M. Oliveira Fernandes Moreira, T. Wlostowski, J. Dedic, C. Prados, M. Kreider, R.Baer, S.Rauch, and T.Fleck, "The white rabbit project," in *Int. Conf. on Accelerator and Large Experimental Physics Control Systems*, Kobe, Japan, 2009.

[8] M. Lipinski, T. Wlostowski, J. Serrano, P. Alvarez, J. Gonzalez Cobas, A. Rubini, and P. Moreira, "Performance results of the first white rabbit installation for cngs time transfer," in *IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS).* IEEE, 2012.

[9] Institute of Electrical and Electronics Engineers, "Time-Sensitive Networking Task Group," 2014. [Online]. Available: http://www.ieee802.org/1/pages/tsn.html

[10] H. Kopetz, *Real-Time Systems : Design Principles for Distributed Embedded Applications.* Springer, 1997.

[11] P. Derler, J. C. Eidson, S. Goose, E. A. Lee, S. Matic, and M. Zimmer, "Using PTIDES and synchronized clocks to design distributed systems with deterministic system-wide timing," in *International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication.* IEEE, 2013.

[12] National Instruments, "LabVIEW RIO Architecture," 2015, http://www.ni.com/white-paper/10894/en/ [Online; accessed 4-August]. [Online]. Available: http://www.ni.com/white-paper/10894/en/

Combinatorial Coverage Analysis of Subsets of the TLS Cipher Suite Registry

Dimitris E. Simos
SBA Research
A-1040 Vienna, Austria
dsimos@sba-research.org

Kristoffer Kleine
SBA Research
A-1040 Vienna, Austria
kkleine@sba-research.org

Rick Kuhn
Computer Security Division
NIST
Gaithersburg, MD, USA
d.kuhn@nist.gov

Raghu Kacker
Applied and Computational
Mathematics Division, NIST
Gaithersburg, MD, USA
raghu.kacker@nist.gov

***Abstract*—We present a combinatorial coverage measurement analysis for (subsets) of the TLS cipher suite registries by analyzing the specified ciphers of IANA, ENISA, BSI, Mozilla and NSA Suite B. The method introduced here may contribute towards the design of quality measures of cipher suites, and may also be applied more broadly to the analysis of configurable systems.**

***Keywords*—Combinatorial testing, coverage, measurement, TLS, subsets, cipher suites.**

I. Introduction

Security protocols continue to suffer from security flaws in their implementations, like the POODLE attack in SSL/TLS or the Heartbleed bug in the OpenSSL cryptographic library. Clearly, additional steps have to be taken to ensure or better contribute towards their quality assurance, as part of the testing cycle where critical points in the system state-space are covered. The full system state-space, consisting of all valid configurations, is generally impossible to cover, because the number of configurations is too large. However, empirical research shows that the number of factors interacting in system failures is relatively small [1]. This has also been confirmed in the case of web application security testing [2].

II. Combinatorial Coverage

Empirical data show that a significant number of software failures are induced by the interaction of two or more factors, and interaction faults can be extremely difficult to identify. Thus it is useful to measure the proportion of 2-way, 3-way, and higher strength combinations that are covered by a test set. Any combinations that have not been tested represent a portion of the input space for which the application has not been shown to be correct. Measuring the proportion of the input space for which the system response is untested and unknown can thus provide a useful quantity in estimating residual risk after testing. We explain the concept of combinatorial coverage measurement, a variety of measures that are available, and theorems relating (static) combinatorial coverage to (dynamic) structural coverage. These concepts are illustrated with examples comparing measures of tests for a NASA spacecraft and open source test configurations for the TLS cipher suite, which is the main focus of this paper.

A configuration with n variables contains $\binom{n}{t}$ t-way combinations, so a test set with many configurations will contain a large number of combinations. *Combinatorial coverage* measures the inclusions of t-way combinations in a test set. Note that this measure is different from conventional structural coverage metrics (such as statement or branch coverage) and is independent of these other measures. Because combinatorial coverage measures the input space that is tested, and consequently also the untested portion of input space, it is a useful in gauging the residual risk after testing. A variety of combinatorial coverage measures are available, including a fundamental measure of *total variable-value configuration coverage*: for a given combination of t variables, the proportion of all t-way value settings that are covered by at least one test case in a test set [3].

For example, two binary variables have four possible settings. Consider four tests containing variables a, b, c, and d: $\{0000, 0110, 1001, 0111\}$. There are $\binom{4}{2} = 6$ possible variable combinations and $2^2 \times \binom{4}{2} = 24$ possible variable-value configurations. Of these, 19 variable-value configurations are covered and the only ones missing are $ab = 11$, $ac = 11$, $ad = 10$, $bc = 01$, $bc = 10$, so the total variable-value configuration coverage is 19/24 = 79%. These measures are shown in Figure 1, where the upper right-hand corner represents the 21% of the 2-way combinations in the input space not tested. Figure 2 shows measurements for 2-way through 5-way combination coverage for 7,489 tests for a NASA spacecraft. Note that the untested portion for 2-way combinations (above red line) is only about 6% of the total, and 3-way to 5-way coverage is relatively high. In contrast, as we shall see shortly after the situation changes rapidly when measuring the combination coverage for the TLS cipher suites.

III. Input Models for Cipher suites

A cipher suite is a combination of key exchange, authentication, encryption and MAC algorithms which are used together to provide the security of TLS. For example, the cipher suite `TLS_RSA_WITH_AES_256_GCM_SHA384` specifies that session secrets are exchanged using RSA while AES with a 256 bit key is used for encrypting the application data and integrity is provided by SHA384. These combinations are specified in various RFCs. For example, NSA Suite B (before a 2015 revision) consisted of the 2 cipher suites `TLS_ECDHE_ECDSA_AES_128_GCM_SHA256` and `TLS_ECDHE_ECDSA_AES_256_GCM_SHA384`. We have developed an input parameter model (IPM) for splitting the suites into parameters (Table XI). It is revealed that 2-way

Simos, Dimitris; Kleine, Kristoffer; Kuhn, David; Kacker, Raghu.
“Combinatorial Coverage Analysis of Subsets of the TLS Cipher Suite Registry.”
Paper presented at the High Confidence Software and Systems Conference, Annapolis, MD, May 10-May 12, 2016.

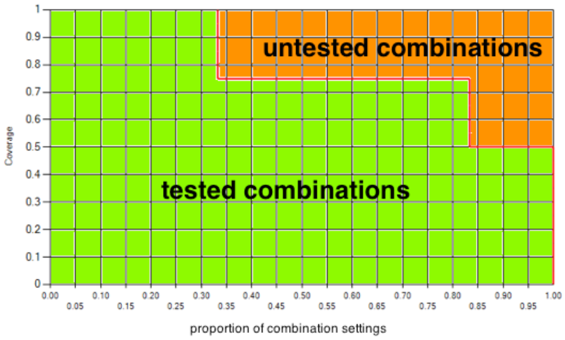


Fig. 1: Example test set

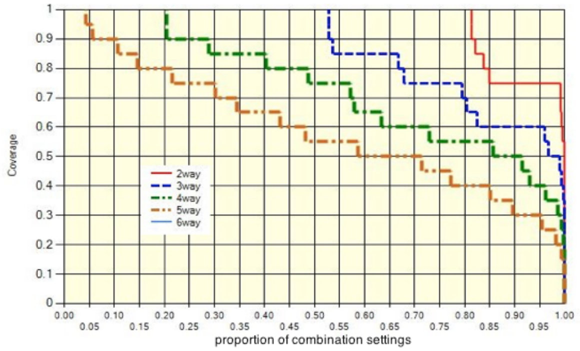


Fig. 2: Measured combinatorial coverage for 7,489 tests.

coverage is achieved for all pairs of parameters except for the parameter pair (Key size, MAC) where the tuples (256, SHA256) and (128, SHA384) are missing.

In addition, we have performed a comparison of the specified cipher suites of IANA, ENISA, BSI, Mozilla and NSA Suite B and our measurement results are given in Table XII. Note that TLS is used only as an illustration of the analysis method, because complex constraints embedded in the TLS code of different implementations have not been included.

For example, if encryption is selected as NULL in the IANA cipher suites, then the key length must be zero and the mode must be NULL as well. Similarly, when the AES key size is 128 bits in NSA suite B, then the hash function must be SHA-256 with 128-bit collision resistance to match the security strength; and when different curves are used with ECDHE_ECDSA, key lengths must be changed. The figures in Table XII can therefore be considered *upper bounds rather than exact sizes of the configuration spaces*. A complete analysis including specific TLS constraints can be considered in a future paper.

A. IANA

The Internet Assigned Numbers Authority (IANA) records all cipher suites which have been specified for TLS (versions 1.0, 1.1 and 1.2) and each cipher suite is assigned a unique identifier (2-byte value).[1] The whole cipher suite list contains 317 cipher suites which are omitted for space reasons, but we give the resulting IPM in Table I. In the context of this paper, we consider a cipher suite list as a test set.

KEX	Enc	Key size	Mode	Hash
NULL	NULL	0	NULL	NULL
RSA	RC4	40	CBC	MD5
RSA_EXPORT	RC2	56	EDE_CBC	SHA
DH_DSS_EXPORT	IDEA	128	GCM	SHA256
DH_DSS	DES	168	CCM	SHA384
DH_RSA_EXPORT	3DES	256	CCM_8	
DH_RSA	AES			
DHE_DSS_EXPORT	CAMELLIA			
DHE_DSS	SEED			
DHE_RSA_EXPORT	ARIA			
DHE_RSA				
DH_anon_EXPORT				
DH_anon				
KRB5				
KRB5_EXPORT				
PSK				
DHE_PSK				
RSA_PSK				
ECDH_ECDSA				
ECDHE_ECDSA				
ECDH_RSA				
ECDHE_RSA				
ECDH_anon				
SRP_SHA				
SRP_SHA_RSA				
SRP_SHA_DSS				
ECDHE_PSK				
PSK_DHE				

TABLE I: IANA IPM

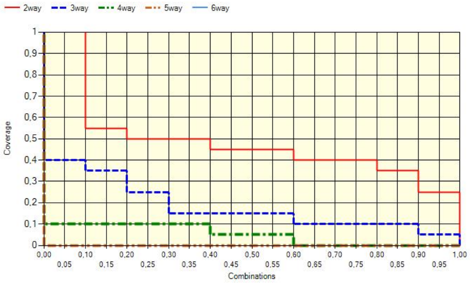


Fig. 3: Coverage IANA

1) Key length constraints:

- For each encryption algorithm one constraint for allowed key sizes (e.g. AES ⇒ key size = 128 or 256)
- Only necessary for IANA model since the other subsets don't allow for invalid combinations

B. ENISA

The following recommendation is issued by the ENISA (European Union Agency for Network and Information Security). The recommendation notes that none of the available key exchange mechanisms are particularly favorable for future use (long term) as no proof of security exists, but recommends (EC)DHE together with RSA, DSS or ECDSA for legacy use as this provides forward secrecy [2]. See Table II for the whole list of cipher suites.

[1] https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4

[2] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/study-on-cryptographic-protocols/at%5fdownload/fullReport

KEX	Enc	Key size	Mode	Hash
DHE_DSS	CAMELLIA	128	GCM	SHA256
DHE_DSS	AES	128	GCM	SHA256
DHE_DSS	CAMELLIA	256	GCM	SHA384
DHE_DSS	AES	256	GCM	SHA384
DHE_RSA	CAMELLIA	128	GCM	SHA256
ECDHE_RSA	CAMELLIA	128	GCM	SHA256
DHE_RSA	AES	128	GCM	SHA256
ECDHE_RSA	AES	128	GCM	SHA256
DHE_RSA	CAMELLIA	256	GCM	SHA384
ECDHE_RSA	CAMELLIA	256	GCM	SHA384
DHE_RSA	AES	256	GCM	SHA384
ECDHE_RSA	AES	256	GCM	SHA384
DHE_RSA	AES	128	CCM	SHA256
DHE_RSA	AES	128	CCM_8	SHA256
DHE_RSA	AES	256	CCM	SHA256
DHE_RSA	AES	256	CCM_8	SHA256
ECDHE_ECDSA	CAMELLIA	128	GCM	SHA256
ECDHE_ECDSA	AES	128	GCM	SHA256
ECDHE_ECDSA	CAMELLIA	256	GCM	SHA384
ECDHE_ECDSA	AES	256	GCM	SHA384
ECDHE_ECDSA	AES	128	CCM	SHA256
ECDHE_ECDSA	AES	128	CCM_8	SHA256
ECDHE_ECDSA	AES	256	CCM	SHA256
ECDHE_ECDSA	AES	256	CCM_8	SHA256

TABLE II: ENISA recommended cipher suites

KEX	Enc	Key size	Mode	Hash
ECDHE_ECDSA	AES	128	GCM	SHA256
ECDHE_RSA	CAMELLIA	256	CCM	SHA384
DHE_RSA			CCM_8	
DHE_DSS				

TABLE III: ENISA IPM

C. BSI

The BSI, a German Federal Agency responsible for computer and network security, gives out recommendations for cipher suites it considers secure to use. See table IV for a full list of these cipher suites. [3]

D. Mozilla

Mozilla recommends specific cipher suites for server side TLS as a guideline for helping system administrators harden the configuration of servers, most notably webservers [4]. We analysed the recommended cipher list for modern compatibility. See table VI for a full list of cipher suites.

[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?%5f%5fblob=publicationFile&v=1

[4] https://wiki.mozilla.org/Security/Server_Side_TLS

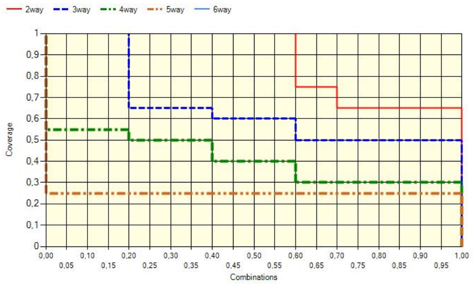


Fig. 4: Coverage ENISA

KEX	Enc	Key size	Mode	Hash
ECDHE_ECDSA	AES	128	CBC	SHA256
ECDHE_ECDSA	AES	256	CBC	SHA384
ECDHE_ECDSA	AES	128	GCM	SHA256
ECDHE_ECDSA	AES	256	GCM	SHA384
ECDHE_RSA	AES	128	CBC	SHA256
ECDHE_RSA	AES	256	CBC	SHA384
ECDHE_RSA	AES	128	GCM	SHA256
ECDHE_RSA	AES	256	GCM	SHA384
DHE_DSS	AES	128	CBC	SHA256
DHE_DSS	AES	256	CBC	SHA256
DHE_DSS	AES	128	GCM	SHA256
DHE_DSS	AES	256	GCM	SHA384
DHE_RSA	AES	128	CBC	SHA256
DHE_RSA	AES	256	CBC	SHA256
DHE_RSA	AES	128	GCM	SHA256
DHE_RSA	AES	256	GCM	SHA384

TABLE IV: BSI recommended cipher suites

KEX	Enc	Key size	Mode	Hash
ECDHE_ECDSA	AES	128	CBC	SHA256
ECDHE_RSA		256	GCM	SHA384
DHE_RSA				
DHE_DSS				

TABLE V: BSI IPM

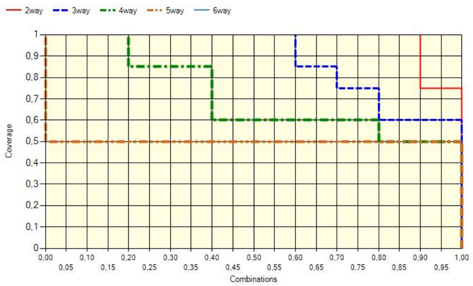


Fig. 5: Coverage BSI

KEX	Enc	Key size	Mode	Hash
ECDHE_ECDSA	AES	128	CBC	SHA
ECDHE_ECDSA	AES	256	CBC	SHA
ECDHE_RSA	AES	128	CBC	SHA
ECDHE_RSA	AES	256	CBC	SHA
ECDHE_ECDSA	AES	128	CBC	SHA256
ECDHE_ECDSA	AES	256	CBC	SHA384
ECDHE_RSA	AES	128	CBC	SHA256
ECDHE_RSA	AES	256	CBC	SHA384
ECDHE_ECDSA	AES	128	GCM	SHA256
ECDHE_ECDSA	AES	256	GCM	SHA384
ECDHE_RSA	AES	128	GCM	SHA256
ECDHE_RSA	AES	256	GCM	SHA384
DHE_RSA	AES	128	CBC	SHA
DHE_DSS	AES	256	CBC	SHA
DHE_RSA	AES	256	CBC	SHA
DHE_DSS	AES	128	CBC	SHA256
DHE_RSA	AES	128	CBC	SHA256
DHE_RSA	AES	256	CBC	SHA256
DHE_RSA	AES	128	GCM	SHA256
DHE_RSA	AES	256	GCM	SHA384
DHE_DSS	AES	128	GCM	SHA256
DHE_DSS	AES	256	GCM	SHA384

TABLE VI: Mozilla recommended cipher suites

KEX	Enc	Key size	Mode	Hash
ECDHE_ECDSA	AES	128	CBC	SHA
ECDHE_RSA		256	GCM	SHA256
DHE_RSA				SHA384
DHE_DSS				

TABLE VII: Mozilla IPM

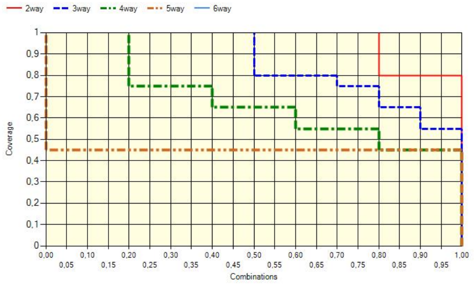


Fig. 6: Coverage Mozilla

KEX	Enc	Key size	Mode	Hash
ECDHE_ECDSA	AES	128	GCM	SHA256
		256		SHA384

TABLE X: NSA IPM (before revision)

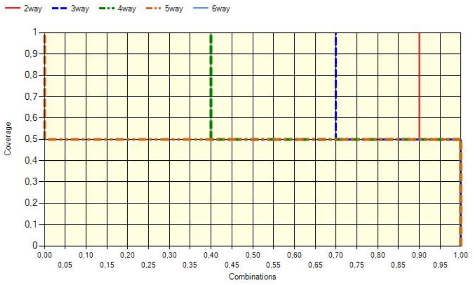


Fig. 7: Coverage NSA Suite B

E. NSA Suite B

Suite B is a recommendation by the NSA [5]. Currently only one cipher, namely `TLS_ECDHE_ECDSA_AES_256_GCM_SHA384`, is recommended. Before a revision in 2015 AES 128 and SHA256 were also allowed.

IV. Measuring TLS Cipher Suites

The TLS cipher suites can be viewed as a collection of configuration settings or options, conditioned that an input parameter model is available. A particular implementation is composed from a number of modules or components that together provide desired functionality. For TLS, the components are of the five types of modules described earlier in Section III. Combination coverage is of interest for configurable systems because interactions between multiple components are often the source of bugs and vulnerabilities. The more potential interactions, the greater the possibility for such interoperability problems, and thus the greater need for testing. The significance of t-way combinations of configuration options is dependent on the application. For TLS cipher suites, an example might be the importance of analyzing the existing pairs of encryption and authentication functions. If encryption is provided without authentication, or with inadequately secure authentication, then users will be vulnerable to a man-in-the-middle attack.

KEX	Enc	Key size	Mode	Hash
ECDHE_ECDSA	AES	128	GCM	SHA256
ECDHE_ECDSA	AES	256	GCM	SHA384

TABLE VIII: NSA recommended cipher suites before 2015 revision

KEX	Enc	Key size	Mode	Hash
ECDHE_ECDSA	AES	256	GCM	SHA384

TABLE IX: NSA recommended cipher suite after 2015 revision

If we wish to analyze a cipher suite, one consideration is the extent to which we can measure combinations of its configurable options. If a new or a revised cipher suite is proposed, for example, interoperability errors may be more common where combinations of options have not been used in the previous versions. For instance, if such a cipher suite has a pair of components that is present in the current suite, then it is already in use and interoperability problems are presumably more likely to have been identified through use. If a particular combination of components was not present in the current implementation, then, in the case that a testing procedure can be applied, this is likely to be required to ensure correct operation than if the current suite already has this pair. Furthermore, if an existing configuration uses both components, then previous test sets should have covered this pair. By identifying pairs and higher strength t-way combinations that are not covered in the current test set, we can improve the test sets by covering the previously untested interactions.

Consider Table II for example. The ENISA cipher suite input model has a configuration of $2^3 3^1 4^1$, for 96 possible implementations. Table XII contains 24 rows, so many other implementations are possible using software for each of the parameters in the input model. Table XII shows that 86% of the pairs have been covered in the ENISA specification, so problems that are related to unspecified 2-way interactions are relatively unlikely if a new option is afterwards added to a revised ENISA cipher suite.

The IANA cipher suite list, on the other hand, has an enormous possible configuration space, with an input model of $5^1 6^2 10^1 28^1$ = 8400 possible implementations. As shown in Table XII, only 45% of the pairs, and only 16% of 3-way combinations are present in the current list. Thus changes or additions are more likely to introduce combinations that have not been used in the existing test sets.

All data can be found in Table XII and is further visualized in Figures 3, 4, 5, 6 and 7 which show the coverage for the IANA, ENISA, BSI, Mozilla and NSA test sets. These figures

[5] https://tools.ietf.org/html/rfc6460

Key exchange	Enc	Key size	Mode	MAC
ECDHE_ECDSA	AES	128	GCM	SHA256
ECDHE_ECDSA	AES	256	GCM	SHA384

TABLE XI: Test set for NSA Suite B

t	IANA	ENISA	BSI	Mozilla	NSA
2	45.55%	86.36%	97.83%	96.36%	89.47%
3	15.51%	65.24%	86.96%	82.5%	76.00%
4	5.41%	43.0%	69.32%	63.71%	62.50%
5	2.52%	25.0%	50.00%	45.83%	50.00%

TABLE XII: Combinatorial coverage ($t \in \{2, 3, 4, 5\}$)

show the proportion of combinations which are covered to a certain extent. For example, in Figure 6 we can see that 50% of all 3-way parameter combinations are fully covered while 70% are covered with at least 80%, and so on.

As noted previously, increasing the number of potential interactions between components may also increase the risk of bugs or vulnerabilities arising from feature interactions. Notice that the NSA Suite B specification contained only two configurations in the past, and now only one, thus limiting the potential for unknown interactions.

V. Cross coverage

We can consider the idea of cross coverage, where coverage is computed for one test array, A, using an input model, M', for a different array, A' of the same kind. That is, the measures produced give the coverage of M' by the tests in A. To the best of our knowledge, the idea of cross coverage is new and it has not been investigated elsewhere. Properties associated with this construct are topics for future papers, but we can review some implications with respect to applications, using the figures shown in Table XII and Table XIII.

Table XII shows the coverage of the five different input models in the header line by their respective cipher suites. For example, the IANA cipher suite covers 46% of the potential 2-way interactions among its components. As noted earlier, TLS is being used here only as an illustration of the analysis method, and constraints (on the related input models) have not been included in the measurement.

In Table XIII, the other four suites are measured in their coverage of the IANA input model. Thus the potential interactions among components of the ENISA suite are 5.8%. Of all the 2-way interactions that could be constructed among the components of the IANA input model, the IANA cipher suite covers 46%, and the ENISA suite covers 5.8%. If potential interactions are a source of problems, and thus represent a need for testing, then we can infer that less testing will be required when constructing an ENISA test set from the individual components for encryption algorithm, mode, etc. than for constructing an IANA test set.

VI. Conclusion and Future Work

In this work, we presented an analysis of the combinatorial coverage of subsets of the TLS cipher suite registry. This analysis was made feasible with the aid of an input model we developed for this cause. Our measurement results (with respect to the input model) indicate that there is a vast number of uncovered configurations in the specified cipher suites for TLS. However, complex TLS code constraints have not been included in this measurement and hence our results should be interpreted as upper bounds rather than exact sizes of the specific configuration spaces.

t	ENISA	BSI	Mozilla	NSA
2	5.83%	4.60%	5.42%	1.74%
3	1.57%	1.17%	1.49%	0.28%
4	0.46%	0.33%	0.43%	0.05%
5	0.19%	0.13%	0.17%	0.02%

TABLE XIII: Cross coverage with IANA IPM ($t \in \{2, 3, 4, 5\}$)

Whether we can view these measurement results as an indication for the root cause of security vulnerabilities is an important research topic that needs to be addressed further. In future work, we plan to undertake measures towards this direction by examining the relation of uncovered configurations and "weak" cipher suites, in the sense of the security strength these ciphers provide, in real data sets for TLS. Within this line of research, it would be also interesting to simulate a similar analysis for cipher suite lists that have been deprecated in newer TLS versions.

Acknowledgment

The research presented in the paper has been funded in part by the Austrian Research Promotion Agency (FFG) under grant 851205 (Security ProtocoL Interaction Testing in Practice - SPLIT) and the Austrian COMET Program (FFG).

Disclaimer: *Products may be identified in this document, but identification does not imply recommendation or endorsement by NIST, nor that the products identified are necessarily the best available for the purpose.*

References

[1] D. R. Kuhn, D. R. Wallace, and A. M. Gallo, Jr., "Software fault interactions and implications for software testing," *IEEE Trans. Softw. Eng.*, vol. 30, no. 6, pp. 418–421, Jun. 2004.

[2] B. Garn, I. Kapsalis, D. E. Simos, and S. Winkler, "On the applicability of combinatorial testing to web application security testing: A case study," in *Proceedings of the 2nd International Workshop on Joining AcadeMiA and Industry Contributions to Testing Automation (JAMAICA'14)*. ACM, 2014.

[3] D. Kuhn, I. Dominguez Mendoza, R. Kacker, and Y. Lei, "Combinatorial coverage measurement concepts and applications," in *Software Testing, Verification and Validation Workshops (ICSTW), 2013 IEEE Sixth International Conference on*, March 2013, pp. 352–361.

Optical system design for femtosecond-level synchronization of clocks

Laura C. Sinclair[1], William C. Swann[1], Jean-Daniel Deschênes[1,2], Hugo Bergeron[1,2], Fabrizio R. Giorgetta[1], Esther Baumann[1], Michael Cermak[1], Ian Coddington[1], and Nathan R. Newbury[1]
[1]National Institute for Standards and Technology, 325 Broadway, Boulder, CO 80305
[2]Université Laval, 2325 Rue de l'Université, Québec, QC, G1V 0A6, Canada

ABSTRACT

Synchronization of optical clocks via optical two-way time-frequency transfer across free-space links can result in time offsets between the two clocks below tens of femtoseconds over many hours. The complex optical system necessary to support such synchronization is described in detail here.
Work of the U.S. government, not subject to copyright.

Keywords: optical two-way time-frequency transfer, optical synchronization, optical metrology, frequency comb

1. INTRODUCTION

Recently, we have demonstrated the tight synchronization of two optical clocks to within femtoseconds across a 4 km turbulent air path.[1] To achieve this level of performance, we use optical two-way time-frequency transfer (O-TWTFT) which removes the picosecond-level turbulence-induced timing fluctuations present on a one-way measurement to achieve femtosecond-level synchronization. Here, we will discuss the optical system design which makes this performance possible.

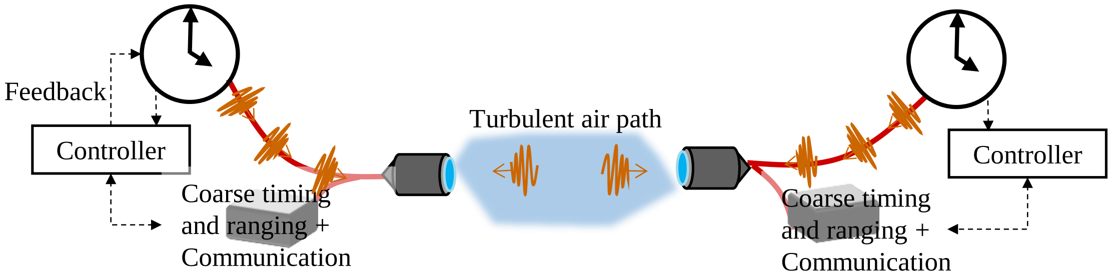


Figure 1. Overview of synchronization system. The coherent pulse train generated by the clock is combined with a coarse timing and communications signal before being launched over the turbulent air path. The arrival of the coherent pulse train (clock signal) from each site is detected with femtosecond precision at the other site. The coarse timing accounts for any ambiguities associated with the separation between coherent pulses, while the communications signal allows for real time computation of the clock difference at the remote site. Feedback is then applied to the remote clock to maintain synchronization between the two clocks, i.e. a time offset of zero at a chosen reference plane.

Figure 1 shows a simplified schematic of the overall O-TWTFT system. Tight synchronization of two clocks to within femtoseconds via O-TWTFT requires five basic steps:

1. The "ticks" of the optical clock must be generated with low pulse-to-pulse timing jitter, which requires an optical oscillator (cavity stabilized laser) and associated phase-locked frequency comb.
2. The timing signal must be sent from one site to the other site and detected with femtosecond precision. As the name suggests, for O-TWTFT, the transfer of clock signals must be bi-directional to cancel fluctuations due to turbulence and platform motion.
3. The timing signals recorded at the master site must be communicated to the remote site. (Here, we refer to the actively synchronized clock as the remote clock.)
4. Based on the two-way timing signals, the controller at the remote site must compute the time offset between the two clocks in realtime.

5. Feedback must be applied to the remote clock to drive the computed time offset between the two clocks to zero at the chosen reference plane.

In O-TWTFT, two different sets of bi-directional timing signals are transmitted, one via frequency comb pulses and one via an rf phase-modulated optical-carrier-wave. This optical carrier wave is also used to transmit the timing information from the master site back to the remote site (step 3 above).

To demonstrate O-TWTFT, a test system was setup at the NIST campus in Boulder, Colorado. This O-TWTFT achieved femtosecond-level synchronization over days.[1] As shown in Figure 2, the hardware is installed in a rooftop laboratory with a folding mirror located 1 km distant on a mesa. Utilization of a twice-folded optical path creates a 4 km path and allows for verification. (See Figure 2.) Indeed, it is critical to configure the system in this way, rather than the point-to-point link of Figure 1, in order to verify synchronization via a separate out-of-loop measurement over a short fiber path that directly connects the two clocks.

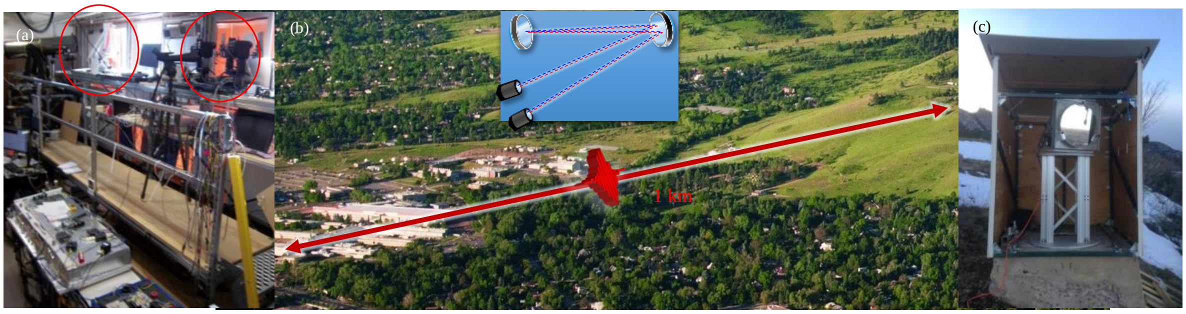


Figure 2. (a) Image of rooftop laboratory with most of the hardware including the free-space optical terminals (red circle) and second folding mirror (red circle). (b) Image of path between rooftop laboratory and first folding mirror on the mesa. Inset shows two-fold optical path geometry used to reach 4 km optical pathlength. (c) Image of first folding mirror on mesa 1 km distant from rooftop laboratory.

The remainder of this paper discusses the optical system. Section 2 provides an overview of the whole system. Section 3 covers the frequency-comb-based optical two-way time-frequency transfer, including the detection of pulse arrival times with femtosecond resolution. Section 4 contains a brief discussion of the sub-nanosecond ‘coarse’ timing and ranging as well as the optical communications link necessary for real-time processing of the timing signals. Section 5 describes the low-insertion loss free-space optical terminals which are used to launch and receive the optical signals. Finally, Section 6 provides details on the synchronization verification. We note that the system described here synchronizes two optical clocks; however, many elements of this system can also be used for the synchronization of a microwave clock to an optical clock.

2. OVERVIEW OF PHYSICAL SYSTEM

The optical system as implemented is quite complex and involves two optical cavities, three frequency combs, six cw lasers, two Doppler-cancelled fiber links, three optical heterodyne detection modules, and two free-space optical terminals. (The digital signal processing and control, which is not described here, has similar complexity including a total of nine servo loops.) Figure 3 gives a more detailed overview of the system.

On each end of the link, a frequency comb is phase-locked to a cavity-stabilized laser located in a separate laboratory. On the master site, a transfer comb is also needed to measure the time offsets at the necessary femtosecond resolution. A multi-function heterodyne module is associated with each of the three frequency combs for the detection of time offsets and stabilization of the comb. Each site has a modulated cw laser for coarse ranging and for communications which is wavelength multiplexed with the comb light launched from the free-space optical terminals. A field-programmable-gate-array-based (FPGA-based) controller at each site performs the real-time processing of comb and cw laser timing signals and generates the feedback signals necessary for closing the synchronization loop.

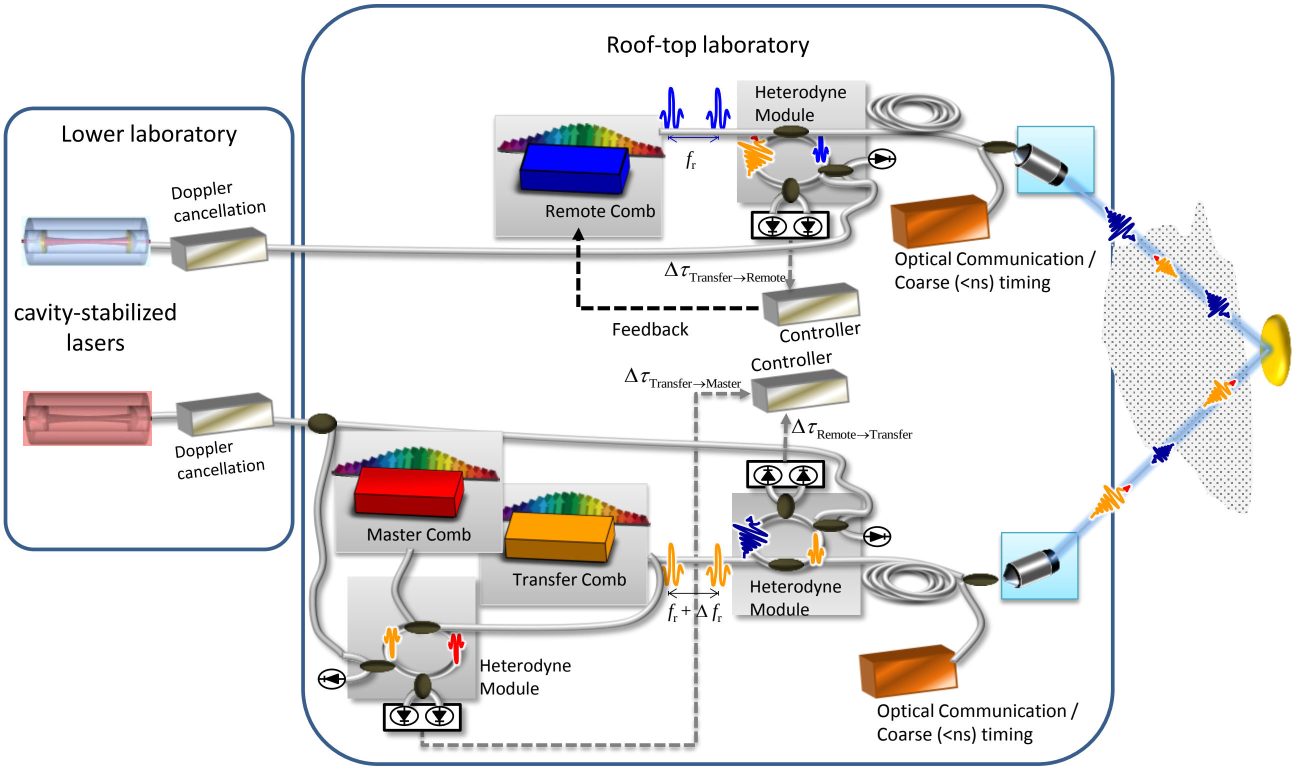


Figure 3. Schematic of synchronization system highlighting the physical system. On the master site, a second transfer comb is implemented for detection of time offsets at the femtosecond level as discussed in Section 2.2 and Section 3.1. The optical cavities and cavity-stabilized lasers are located in a separate laboratory and connected via Doppler-cancelled fiber links. The multi-function heterodyne modules contain elements for launching comb light across the link, detecting the incoming timing signals, and phase-locking the frequency combs to the cavity-stabilized lasers. The optical path is folded to allow for synchronization verification. (One potential source of confusion is that sub-systems within a clock site are often tightly coupled physically to avoid systematic timing drifts even if they might be separated in a conceptual diagram. For instance the heterodyne module both detects the optical signal to phase-lock the frequency comb to the cavity stabilized laser and detects the timing signals from the incoming optical pulse train.)

Before discussing the design of the optical subsystems in more detail, we discuss two important underlying operations: the generation of the optical timescale at each site and the calculation of the overall master synchronization equation.

2.1 Generating a Clock Output

At both the master and remote site, we must construct a clock. Here, we do so by tightly phase-locking a frequency comb to a cavity-stabilized laser. The frequency comb at each site coherently converts the ~100 THz optical frequency of the cavity-stabilized laser to the more accessible "clock tick" comb repetition frequency of ~200 MHz. (See Figure 4.) The time output of the clock then consists of the labeled pulse train generated by the frequency comb with the time defined by the arrival of a pulse at a chosen reference plane. When operating synchronously, the repetition frequency for the master and remote combs are identical and the two pulse trains overlap at a common reference plane. Note that for continuous time output, as opposed to the more standard frequency output, the combs cannot exhibit any phase-slips.

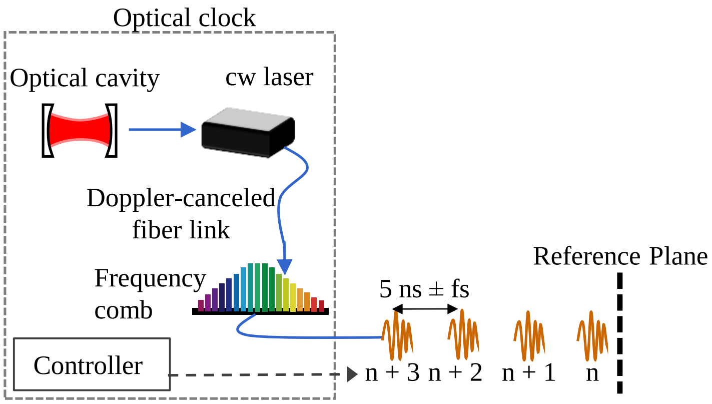


Figure 4. Optical clock structure at each site. A single comb tooth of a self-referenced frequency comb[2] is phase-locked to a cavity-stabilized cw laser. A Doppler-cancelled fiber link connects the cw laser to the frequency comb as they are separated by ~ 400 m. A controller labels the pulses of the 200-MHz-repetition-frequency comb. The comb pulses have only a few femtoseconds of pulse-to-pulse timing jitter. The time is defined when the labeled pulses cross a chosen reference plane. The position of the reference plane must be set in a calibration step.

For our system, the high performance optical cavity essentially serves as the frequency reference since the laser frequency follows any variations in the cavity length. For longer term stability or absolute time, the optical cavity could in turn be referenced to an atomic reference. The synchronization measurements should retain the same performance since here we measure the synchronization of the remote clock to the master clock, whatever its timebase.

2.2 Synchronization Equation

In the introduction, we gave a top level discussion of the synchronization process. As mentioned, it relies on the measurement of two-way timing information between the two sites followed by a calculation of the overall time offset between the clocks based on these measurements. We first provide a simple picture of this two-way time offset measurement before describing the more complicated configuration that applies to O-TWTFT. In the simple picture, we record two time offsets. First, we record the time offset associated with the arrival of a particular pulse from the remote site as measured at the master site, $\Delta\tau_{\text{Remote}\to\text{Master}} = T_{\text{link}} + \Delta T$, where T_{link} is the time-of-flight across the link and ΔT is the clock difference. Second, we record the arrival of a pulse from the master site (with the same nominal time) as measured by the remote site, $\Delta\tau_{\text{Master}\to\text{Remote}} = T_{\text{link}} - \Delta T$. Atmospheric turbulence and platform motion can induce variations in the time-of-flight, T_{link}. However, by taking the difference of these arrival times, T_{link} is removed due to the reciprocity of a single-spatial mode optical link[3] leaving only the clock difference, i.e.

$$\Delta T = \frac{1}{2}\left(\Delta\tau_{\text{Remote}\to\text{Master}} - \Delta\tau_{\text{Master}\to\text{Remote}}\right) \tag{1.1}$$

This is the basic two-way time-frequency picture.

However, direction detection of the comb pulses with femtosecond resolution is not possible and as a consequence we implement the transfer comb as discussed in Section 3.1. Now, three time offsets must be recorded: the arrival of the transfer comb pulses as measured at the remote site, $\Delta\tau_{\text{Transfer}\to\text{Remote}}$, the arrival of the remote comb pulses as measured at the master site (by the transfer comb as described later), $\Delta\tau_{\text{Remote}\to\text{Transfer}}$, and the time offset between the transfer and master comb pulses, $\Delta\tau_{\text{Transfer}\to\text{Master}}$. (See Figure 3.) There are ambiguities associated with each of these time offset measurement because the comb pulses are separated by only $1/f_r$~ 5 nsec; these must be removed by a "coarser" two-way time-frequency measurement. As given in Ref. 1, we have developed a master synchronization equation that combines all these measurements to calculate the time offset between the master and remote clocks, ΔT. This equation is:

$$\Delta T = \frac{1}{2}\left(\Delta\tau_{\text{Remote}\to\text{Transfer}} - \Delta\tau_{\text{Transfer}\to\text{Remote}}\right) - \Delta\tau_{\text{Master}\to\text{Transfer}} + \tau_{\text{cal}} - \left(\frac{\Delta f_{\text{r}}}{2f_{\text{r}}}\right)\left(T_{\text{link}} + \Delta t_{\text{ADC}}\right) + \frac{\Delta n}{2f_{\text{r}}} \quad (1.2)$$

where f_r is the repetition frequency of the master comb, Δf_r is the difference in repetition frequencies between the master and transfer combs, T_{link} is again the time-of-flight across the link, Δt_{ADC} is time offset in the analog-to-digital converters (ADCs) at the two sites, and Δn is an integer associated with the labeling of pules. The first three terms represent the generalized form of Equation 1.1. The next term, τ_{cal}, is a term which accounts for the calibration of fixed delays so that $\Delta T = 0$ at the desired reference plane. The next two terms are suppressed by $\Delta f_r / f_r \sim 1/200,000$ and calculated based on measurements made by the coarse TWTFT measurement (Section 4). They are both a consequence of the necessary offset in repetition frequencies between the transfer and remote comb pulse trains. The final term is the previously mentioned ambiguity. This in-loop time offset ΔT is calculated at the remote site, so that any corrections can be applied to the remote clock. The communications link (see Section 4.2) transmits the necessary time offsets from the master site to the remote site to permit calculation in real time.

In the next section, we discuss implementation of the comb-based two-way time-frequency transfer that yields the values for $\Delta\tau_{\text{Transfer}\to\text{Remote}}$, $\Delta\tau_{\text{Remote}\to\text{Transfer}}$, and $\Delta\tau_{\text{Transfer}\to\text{Master}}$. Section 4 discusses the implementation of the coarse two-way time-frequency transfer that yields values for T_{link}, Δt_{ADC} and τ_{cal}.

3. COMB-BASED OPTICAL TWO-WAY TIME-FREQUENCY TRANSFER

3.1 Overview

The frequency combs produce pulse trains with pulse-to-pulse timing jitter of only a few femtoseconds. Direct detection of the pulses, however, would provide only picosecond resolution; to take advantage of the femtosecond-level comb jitter, we implement a linear optical sampling (LOS)[4] technique that achieves the necessary femtosecond resolution. At each site, the local comb is heterodyned with the received distant comb light. As the two comb's repetition frequencies differ by a few kHz, this generates an interferogram (cross-correlation) on the detector as the comb pulses walk through each other. The time at which the peak of the interferogram arrives, detected with a matched filter approach, then can be mapped onto the time offset between the underlying pulse trains.

There is a trade-off between the interferogram repetition rate, i.e. the offset in repetition frequencies, which sets the update rate of the time offset measurements and the amount of comb spectral bandwidth due to the Nyquist sampling theorem.[4] A lower update rate allows for an increased bandwidth and, potentially, an increased signal-to-noise; however, the lower update rate also lowers the bandwidth of the synchronization feedback. We find that a ~2 kHz offset in repetition frequencies is a nice balance.

This LOS sampling is not done directly between the master and remote comb pulse trains since they operate at the same repetition frequency. Instead, a transfer comb is introduced at the master site that has an offset repetition frequency. In this way, LOS sampling is implemented at each end of the link while allowing the master and remote combs to "tick" at the same rate for optical synchronization. Figure 5 shows an example of measured interferograms between the incoming transfer comb pulse train and master comb pulse train at the master site (left side) and the reverse (right side).

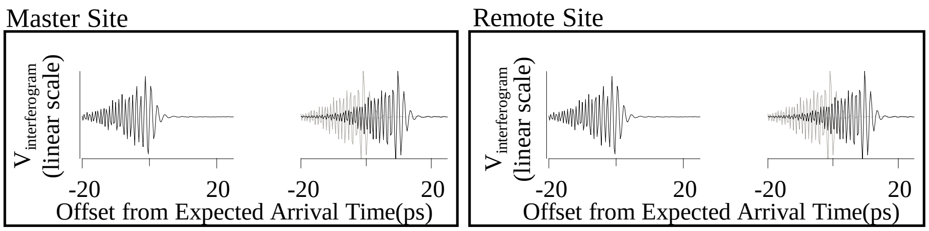


Figure 5. Example of detected interferograms (cross-correlations) at system start and a later time at master and remote sites. The second set of interferograms have a shift from their expected arrival time (gray trace) due atmospheric turbulence. This shift due to turbulence cancels exactly when the difference in arrival times is taken leaving only the clock time offset.

Figure 6 shows the physical implementation of this system at the remote site. The frequency comb at the remote site is housed in two separate aluminum boxes. The optical LOS sampling is implemented in a separate heterodyne detection module. This module actually serves multiple purposes as is discussed in Section 3.6; here, its overlap of the remote comb and incoming transfer comb pulse trains is the relevant function. The photodetected interferogram is digitized at 100 MS/s and processed in the FPGA controller. Other inputs and outputs to the FPGA controller are also noted in Fig. 6b. Note that the heterodyne nature of the LOS measurement also increases the link availability as it detects the incoming pulses near the shot-noise limit. The detection threshold, i.e. the lowest received power for which we can compute a time difference, is only 2 nW (78 photons per pulse). At the master site, the configuration is very similar for the LOS sampling between the incoming remote comb pulse train and local transfer comb pulse train. A second heterodyne module tracks the time offset between the master and transfer comb pulse trains.

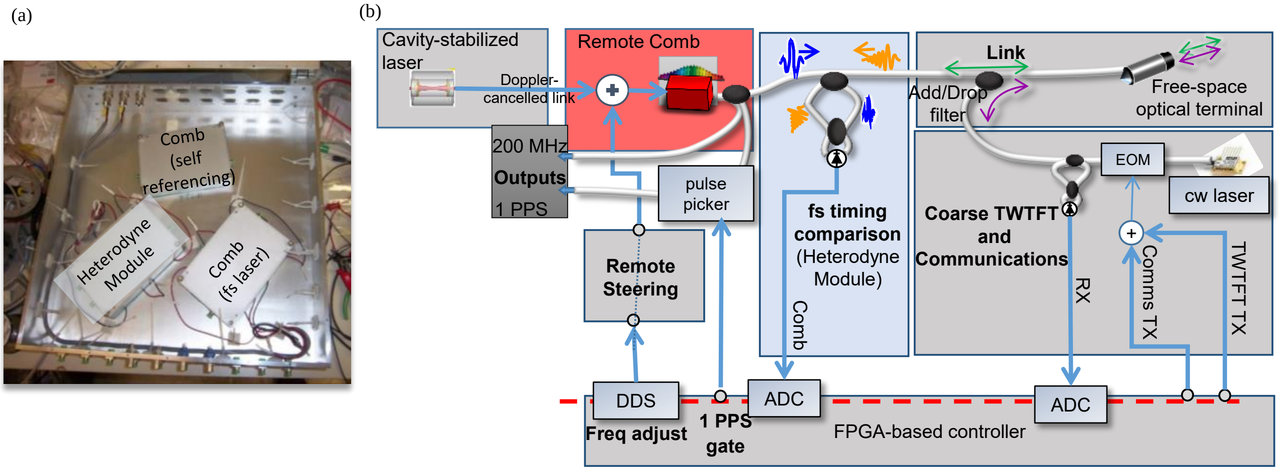


Figure 6. (a) Image of comb (in two boxes) and heterodyne module. (b) Detailed schematic of remote site. The red shaded box indicates the frequency comb of (a) while the blue shaded box contains the heterodyne detection of the interferogram between the transfer and remote combs. The comb light is wavelength multiplexed with the coarse timing and communications signals as shown in the right grey boxes. The FPGA-based controlled modulates the cw laser for the coarse timing and communications, processes both the incoming heterodyne comb signal and incoming modulated cw laser signal, and drives a direct digital synthesizer (DDS) to provide the feedback necessary. The FPGA controller, coarse TWTFT/communication system, and free-space terminal are not shown in Fig. 6a. Comms: communications; RX: receive; TX: transmit; EOM: electro-optic modulator; TWTFT: two-way time frequency transfer; PPS: pulse-per-second; ADC: analog-to-digital converter

In the remainder of this section we discuss the various optical subsystems of Fig. 6 that are involved in the comb-based TWTFT. (The coarse TWTFT, communications and free-space optics terminals are discussed in their own sections.)

3.2 Cavity-Stabilized Lasers and Doppler-Cancelled Links

The cavity-stabilized laser consists of a commercial cw fiber laser locked to an optical cavity yielding a ~1 Hz linewidth and a typical environmentally-induced drift ranging from 0 Hz/s to 10 Hz/s. The cavity-stabilized laser frequency is 195.297,562 THz for the master site, and 195.297,364 THz for the remote site. The cavity-stabilized lasers are located in an environmentally stable lab ~ 400 m away from the rooftop laboratory as the cavities are temperature sensitive. Two separate Doppler-cancelled fiber links transport the stabilized cw light to the location of the frequency combs. The phase-lock of the Doppler-cancelled links is monitored during synchronization to ensure that no phase slips occur.

3.3 Frequency Combs

As noted in the introduction to this section, there are three combs: a remote comb, a master comb, and a transfer comb. All three combs are self-referenced optically-coherent fiber frequency combs with field-programmable-gate-array-based (FPGA-based) digital control and can operate for days without any phase-slips[2]. The 972,920th mode of the master comb is locked to the master cavity-stabilized laser to yield a repetition rate of ~200.733,423 MHz. The 972,909th mode of the transfer comb is similarly locked to the same cavity-stabilized laser to yield a repetition rate that differs by $\Delta f_r = 2.27$ kHz. Note that the ratio $\Delta f_r / f_r \equiv (979{,}920 - 972{,}909)/972{,}920$ is exact and immune to clock drifts. At the remote site, the 972,919th mode of the remote comb is locked to the second cavity-stabilized laser with an rf offset that is ultimately adjusted for synchronization.

The comb design used here follows Ref. 2 , so the comb is actually physically distributed between two aluminum boxes, as shown in Fig. 6a. One box contains the femtosecond fiber laser and an amplifier while a second box contains the optics for the detection of the offset frequency (including nonlinear fiber for supercontinuum generation, periodically poled lithium niobate for frequency doubling of the 2 μm light, and in-line f-to-2f interferometer). The first aluminum box containing the femtosecond laser is temperature controlled and both boxes are located within a larger aluminum enclosure, as shown in Fig. 6a, which is loosely temperature controlled. This temperature control of the femtosecond laser's enclosure is discussed in detail in Section 3.5.

To avoid time variations due to out-of-loop fiber, the optical heterodyne signal between the frequency comb and the cavity-stabilized laser is not detected within either of the two aluminum enclosures housing the comb. Rather the comb light is sent to the heterodyne module (i.e. the third aluminum box in Fig. 6a), where it is finally heterodyned against the cavity-stabilized laser to generate an error signal. This optical heterodyne signal is then sent to the comb's FPGA digital controller along with the offset frequency signal. The FPGA controller then phase-locks the comb output by feedback to the femtosecond fiber laser through pump power and cavity length.

3.4 Comb Signals Launched Across the Link

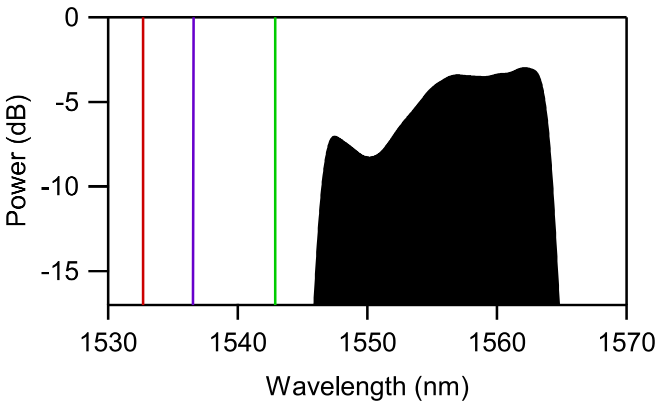


Figure 7. Optical spectrum transmitted across the free-space link. The filtered, transmitted comb spectrum (black shaded region), two modulated cw lasers (purple) at 1536.5 nm, and the two beacon lasers used for the free-space terminals (red and green) at 1532.7 nm and 1542.9 nm.

A portion of the remote and transfer comb spectra is launched across the link, while the remote and master comb pulse trains provide the clock outputs at either site. As discussed in Section 3.1, there is a balance between the rate of time offset measurements and the spectral bandwidth of the comb used for detection. It is not advantageous to try to launch the full 1 μm – 2 μm octave-spanning comb spectrum across the link. Instead, as shown in Figure 7, a 16-nm-wide optical bandwidth centered at 1555 nm out of the comb is launched across the link with a total transmitted power (at the transmit aperture) of ~2.5 mW. The 16-nm bandwidth also leaves additional space in the C-band for the modulated cw laser and beacon lasers without cross-talk between the comb and cw lasers.

3.5 Stabilization of the Comb against Temperature Fluctuations

Temperature control of the frequency combs is critical given their environmentally unstable location. Temperature fluctuations cause changes in the femtosecond fiber laser cavity length and therefore the repetition frequency. To stabilize the cavity length, the digital controller feeds back to piezo-electric transducer (PZT) actuators that are glued to the fiber cavity. However, if the temperature excursions are too large, the resulting cavity length correction can exceed the dynamic range of the PZTs. Their range is limited to ~ 1 μm and thus the temperature of the comb must be well controlled to within 0.1 °C - a factor of ten below that of the laboratory room temperature fluctuations.

To achieve this level of stability, 10 kΩ thermistor is placed in good thermal contact with the inside of the enclosure housing the femtosecond fiber laser. A commercial temperature controller then regulates the enclosure temperature via thermo-electric coolers (TECs) placed below the aluminum enclosure. Because of temperature gradients, the thermistor and the cavity length may not agree on the temperature so serving the cavity length by directly adjusting the temperature is not feasible. We therefore implement a second feedback loop so that when the PZT actuator approaches the edge of its dynamic range, the comb's digital controller adjusts the temperature controller's setpoint by ~ 0.05 °C increments until the PZT actuator returns to the center of its range. This approach has an additional advantage of reduced sensitivity to the performance characteristics of the temperature controller. We use a single point thermistor as our temperature measurement for a dispersed set of fibers and generic Steinhart-Hart coefficients[5] when computing the temperature. Finally, the temperature controller also allows us to coarsely tune the repetition frequency of the comb as the repetition frequency shifts by ~ 2 kHz/°C so that we can coarsely match the repetition frequencies of the master and remote combs before synchronization. Figure 8 shows this operation.

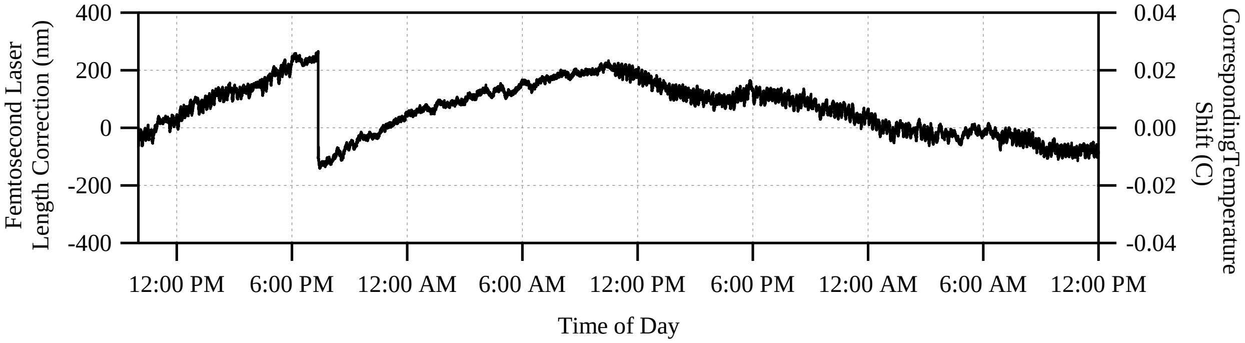


Figure 8. Correction applied to the cavity length of the master frequency comb's femtosecond laser over the 50 hour measurement of Ref. 1. The corresponding calculated temperature shift is given on the right axis. The sharp step after 6:00 pm is a length correction applied by the temperature control module to keep the cavity length within the range of the control actuator. The remaining corrections are applied by the PZT actuators.

3.6 Multi-Function Heterodyne Detection Modules

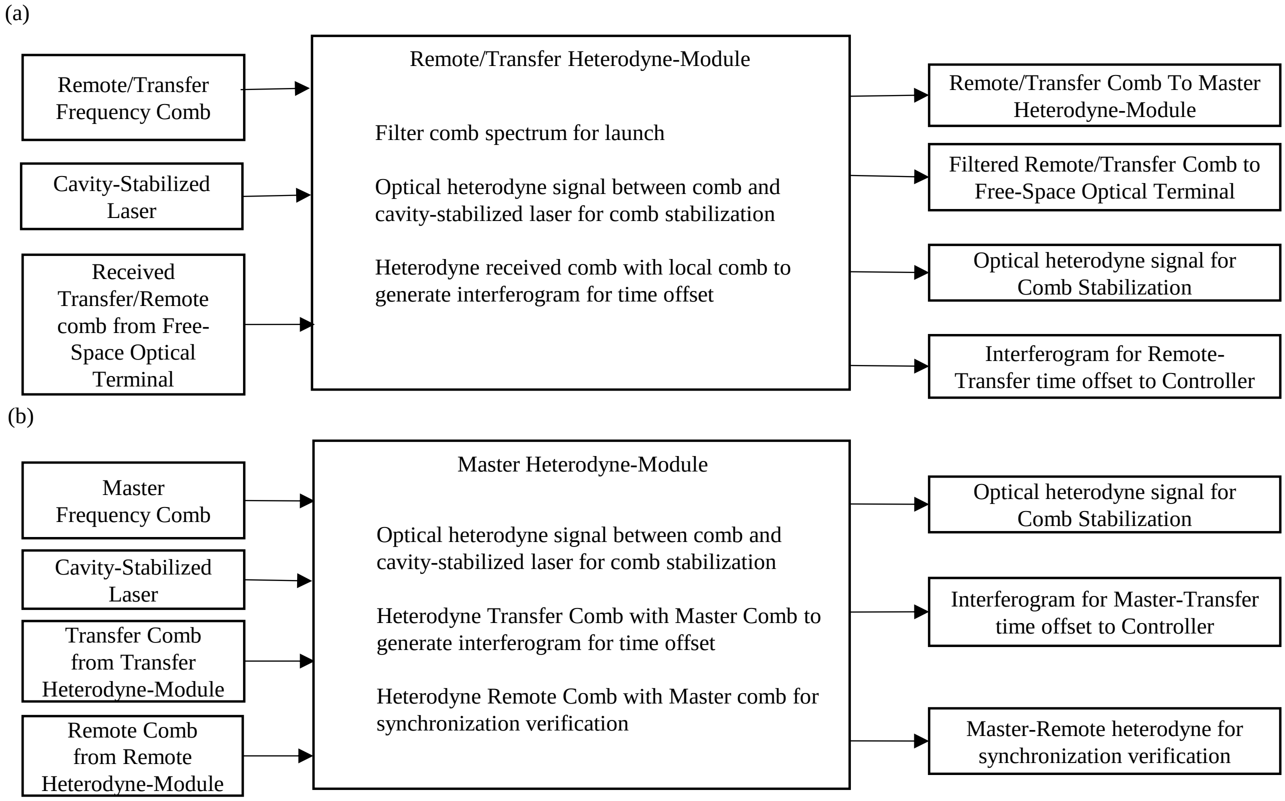

(a)
Remote/Transfer Frequency Comb
Cavity-Stabilized Laser
Received Transfer/Remote comb from Free-Space Optical Terminal
Remote/Transfer Heterodyne-Module
Filter comb spectrum for launch
Optical heterodyne signal between comb and cavity-stabilized laser for comb stabilization
Heterodyne received comb with local comb to generate interferogram for time offset
Remote/Transfer Comb To Master Heterodyne-Module
Filtered Remote/Transfer Comb to Free-Space Optical Terminal
Optical heterodyne signal for Comb Stabilization
Interferogram for Remote-Transfer time offset to Controller
(b)
Master Frequency Comb
Cavity-Stabilized Laser
Transfer Comb from Transfer Heterodyne-Module
Remote Comb from Remote Heterodyne-Module
Master Heterodyne-Module
Optical heterodyne signal between comb and cavity-stabilized laser for comb stabilization
Heterodyne Transfer Comb with Master Comb to generate interferogram for time offset
Heterodyne Remote Comb with Master comb for synchronization verification
Optical heterodyne signal for Comb Stabilization
Interferogram for Master-Transfer time offset to Controller
Master-Remote heterodyne for synchronization verification

Figure 9. Overview of heterodyne modules, their respective inputs (left) and outputs (right), and their functions (center). (a) Design for the Remote Heterodyne-Module and Transfer Heterodyne-Module. (b) Design for the Master Heterodyne-Module.

The remote site includes a single Remote Heterodyne-Module that serves several purposes including detection of the time offset between the incoming transfer comb pulses and remote comb pulses. The master site includes two heterodyne modules: a Transfer Heterodyne-Module and a Master Heterodyne-Module. The Transfer Heterodyne-Module parallels the Remote Heterodyne-Module in that it detects the time offset between the incoming remote comb pulse and transfer comb pulses. The Master Heterodyne-Module detects the time offset between the transfer and master comb pulses. In addition to the time offset detection, the modules contain elements for the phase-locking of the relevant frequency comb to their cavity-stabilized laser. Each heterodyne module and its associated comb is inside an outer enclosure as show in Figure 6a and Figure 13.

Figure 9 shows the full function of each heterodyne module while Figure 10 gives their detailed optical layout. The Remote Heterodyne-Module and Transfer Heterodyne-Module (Figure 9a) have a nearly identical configuration. In both modules, a portion of the comb light is filtered for launch across the link. The received light is then heterodyned with 100 μW of in-band local comb light to create a cross-correlation, or interferogram, for the detection of the time offset between the remote and transfer comb pulse trains (see Figure 5). In addition, the Doppler-cancelled links for the cavity-stabilized lasers terminate in these modules. (At the master site, the cavity-stabilized light is split between the two heterodyne modules.) The Master Heterodyne-Module is similar except it does not send or receive light to the free-space optical terminals and it is also contains the optics for the out-of-loop heterodyne overlap of the remote and master pulses used in the synchronization verification.

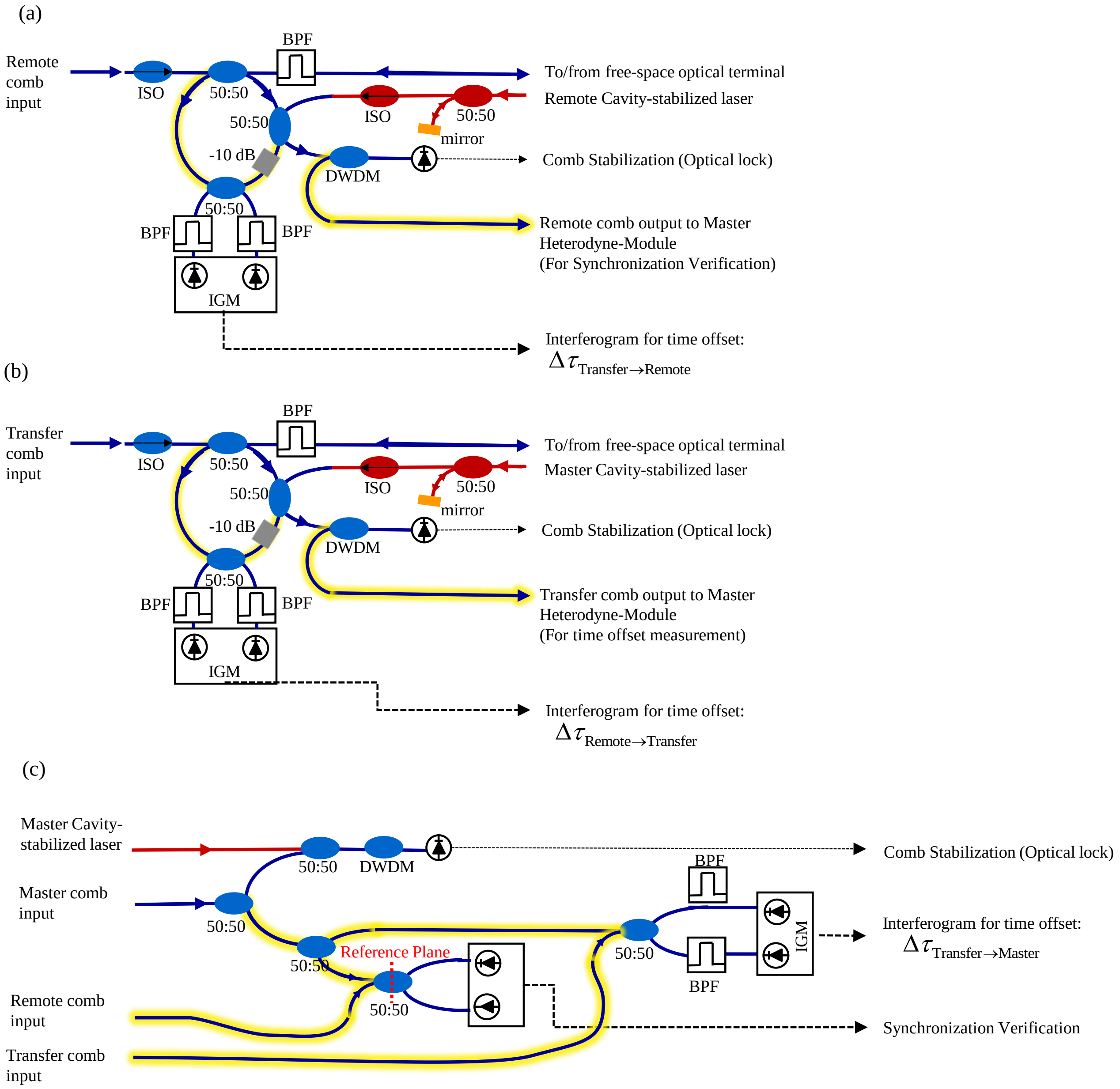

(a)
Remote comb input
ISO
50:50
BPF
50:50
-10 dB
ISO
50:50
mirror
DWDM
To/from free-space optical terminal
Remote Cavity-stabilized laser
Comb Stabilization (Optical lock)
Remote comb output to Master Heterodyne-Module (For Synchronization Verification)
50:50
BPF
BPF
IGM
Interferogram for time offset: $\Delta\tau_{\text{Transfer}\rightarrow\text{Remote}}$
(b)
Transfer comb input
ISO
50:50
BPF
50:50
-10 dB
ISO
50:50
mirror
DWDM
To/from free-space optical terminal
Master Cavity-stabilized laser
Comb Stabilization (Optical lock)
Transfer comb output to Master Heterodyne-Module (For time offset measurement)
50:50
BPF
BPF
IGM
Interferogram for time offset: $\Delta\tau_{\text{Remote}\rightarrow\text{Transfer}}$
(c)
Master Cavity-stabilized laser
50:50
DWDM
Comb Stabilization (Optical lock)
Master comb input
50:50
50:50
Reference Plane
50:50
BPF
BPF
50:50
IGM
Interferogram for time offset: $\Delta\tau_{\text{Transfer}\rightarrow\text{Master}}$
Remote comb input
Transfer comb input
Synchronization Verification

Figure 10. Detailed multi-function heterodyne module schematic. See text for details. (a) Remote Heterodyne-Module design. (b) Transfer Heterodyne-Module design. (c) Master Heterodyne-Module design. Note that the free-space optical terminals (FSO) are both an input and an output. The reference plane for the out-of-loop verification is indicated by a red dashed line in (c). Temperature sensitive fiber paths are highlighted in yellow for (a) – (c). Blue lines: polarization-maintaining fiber; red-lines: single-mode fiber; FSO: free-space optical terminal; BPF: band-pass filter; ISO: optical isolator; DWDM: dense wavelength division multiplexer; IGM: interferogram

3.7 Temperature Stability of Heterodyne Modules

The rooftop laboratory is not an environmentally stable environment. The room temperature can exhibit variations as large as 10 °C as show in Figure 15. There are building vibrations associated with the fifth floor location. Finaly, the humidity is uncontrolled. During the 50-hour measurement of Ref. 1, the room temperature varied by 4 °C and the relative humidity ranged between 13% and 20%. The temperature fluctuations are particularly concerning as these fluctuations can induce fractional optical pathlength variations in fiber paths at approximately 10^{-5}/°C. The effect of relative humidity fluctuations is an order of magnitude lower and thus less of a concern given the usually stable relative humidity in Boulder, Colorado. While the system includes many fiber optic paths, it has been designed such that most fiber paths are either effectively inside the phase-locked loop for the frequency comb stabilization or included in the bidirectional two-way link. Therefore, variations in these fiber paths do not lead to time drifts between the synchronized clocks. However, there are a few fiber paths for which this is not the case. These critical fiber paths are highlighted in yellow in Figure 10. To reduce temperature fluctuations on these critical fiber paths, the heterodyne modules are housed in small aluminum boxes (see Fig. 6a), which are actively temperature controlled at 21.0 °C with a standard deviation of 0.005 °C as measured by the control thermistor. These boxes, along with the associated frequency comb boxes, are housed within a larger outer aluminum enclosure that also has rough temperature control. We measured the temperature sensitivity of the synchronization by monitoring the out-of-loop time offset while deliberating shifting the module temperature by 0.2 °C. For the Master Heterodyne-Module, we recorded a sensitivity of 130 fs/°C, while for the Remote Heterodyne-Module and the Transfer Heterodyne-Module, it was 100 fs/°C.

4. COARSE TWO-WAY TIME-FREQUENCY TRANSFER AND COMMUNICATIONS LINK

As discussed in Section 2.2, the comb-based TWTFT discussed in the previous section yields $\Delta\tau_{\mathrm{Transfer}\rightarrow\mathrm{Remote}}$, $\Delta\tau_{\mathrm{Remote}\rightarrow\mathrm{Transfer}}$, and $\Delta\tau_{\mathrm{Transfer}\rightarrow\mathrm{Master}}$. However, full calculation of the time offset requires a second the coarse two-way time-frequency transfer to provide unambiguous values for T_{link}, Δt_{ADC} and Δn. In addition, the timing information at the master site must be transmitted to the remote site. Both these functions – the measurement of the additional timing quantities and the communications – are provided by the same physical system shown in Figure 11.

In this subsystem, a 1536.5-nm distributed feedback (DFB) laser is followed by a Mach-Zehnder phase modulator, which is controlled by the local FPGA-based synchronization controller to generate an rf phase modulated signal. This signal is wavelength multiplexed with the filtered comb light and transmitted across the link to the opposite site. At the opposite site, this transmitted phase-modulated light is detected by coherent balanced heterodyne detection against the local DFB (unmodulated) cw laser. The two DFB lasers must operate near the same frequency if this coherent heterodyne signal is to be within the detection bandwidth. To this end, the DFB laser at the remote site is frequency-locked to the incoming DFB laser from the master site with a frequency offset of 150 MHz via a frequency-locked loop implemented on the FPGA controller. Use of balanced coherent detection yields high sensitivity and reduces the dynamic range which in turn reduces systematics for TWTFT.

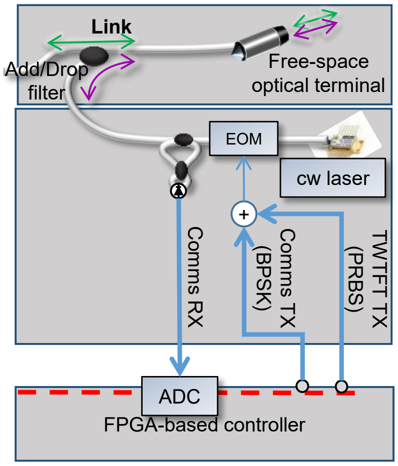


Figure 11. Coarse Two-way Time-Frequency Transfer and Communications on Remote Site. Based on control signals from the FPGA-based controller, an electro-optic phase modulator (EOM) encodes a signal on the cw light with binary phase-shift keying (BPSK). For the coarse timing and ranging, a pseudo-random binary sequence (PRBS) is transmitted. For the communications, data is transmitted. Two 50:50 combiners are used to overlap the local cw laser with the received modulated signal. The resulting heterodyne signal is centered at 150 MHz and is demodulated by the controller to extract the TWTFT timing signal and communications data.

4.1 Coarse Two-Way Time-Frequency Transfer

When the master site detects an overlap (interferogram centerburst) between the incoming remote comb pulse train and transfer comb pulse train, it initiates the 'coarse' timing and communications protocol. The master side first transmits a ~10^4 chips Manchester-coded PRBS at ~100-ns chip length (~10 Mb/s signaling rate). The use of a Manchester-coding allows for a simple and robust implementation. Once this signal is detected at the remote site, the remote site then transmits its own PRBS across the link. Both sites timestamp the arrival of the local and transmitted PRBS according to their respective local timebase. The difference of these timestamps via the analog of equation (1.1) yields the coarse time offset between the ADC clocks, Δt_{ADC} . Since the ADCs are clocked synchronously off the remote and master combs this measurement also yields Δn . Finally, the sum of these timestamps yields the link delay T_{link} This PRBS-based TWTFT has a 40 ps resolution, which is well below the 2.5 ns ambiguity which arises from the 200-MHz repetition frequency of the combs.

4.2 Communications Link

Additionally, after the PRBS signal, the laser is modulated to communicate data between sites. For communication, the system operates in half-duplex mode using Manchester encoded binary phase shift keying (BPSK) at 10 Mbps. The master site uses the communication link to transmit its measured timestamps so that the remote site can use these measurements to independently compute the coarse clock time offset and the coarse time-of-flight across the link. It also sends the results of the comb time offset measurements. This entire protocol of PRBS two-way transfer and communications requires 350 μs of time, or below the interferogram repeat time of $1/\Delta f_r =$ 500 μs.

5. LOW LOSS FREE-SPACE OPTICAL TERMINALS

To provide for reciprocity through the turbulent atmosphere, a single-spatial-mode free-space link must be implemented, essentially requiring that the phase of the received light vary by less than a radian over the receiver aperture. This "coherence size" is a characterized property of coherent light propagating through turbulence[6] and is on the order of a few centimeters for moderate turbulence over km-scale horizontal atmospheric paths. Successful detection of the in-loop time offset requires the received power to be above the detection threshold of a few nanowatts; increasing the received power above this relatively low threshold does not further improve the synchronization. The free-space optical terminals are designed to match the beam diameter to the atmospheric coherence size, to have low insertion loss in order to support the largest range of power fluctuations possible, and to correct for turbulence-induced beam wander.

The zeroth order "piston mode" turbulence effect, given by air density variations (as well as platform sway) that change the optical path length, is removed by the two-way time transfer as it is reciprocal for a single-spatial-mode link. However, the first order beam wander can strongly limit link availability if uncorrected. By applying a first order tip/tilt correction on the free-space optical terminals at both sites, we can achieve average link availabilities on average of 85% across a 4 km link close to the ground in Boulder, Colorado.

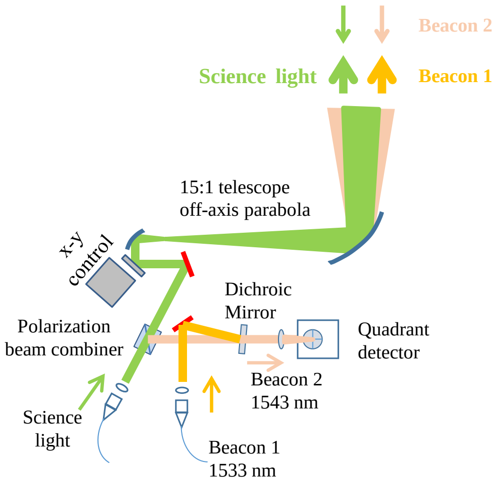


Figure 12. Detailed schematic of low insertion loss free-space optical terminal. See text for details.

The terminal design is shown in Figure 12. The terminal serves to both launch light across the link and receive light from the far end of the link, and as such are fully bi-directional. The combined 'science' light of the comb and modulated cw laser is launched from single mode fiber at the input of the free-space terminal. This light is then polarization multiplexed with a beacon laser. The beacon lasers are selected to not interfere with the science light and are at wavelengths of 1532.7 nm and 1542.9 nm for the two terminals. (See optical spectrum in Figure 7.) The combined beam is then directed off a fast galvanometric steering mirror, expanded in an off-axis, reflective parabolic telescope, and launched over free space. The beacon lasers have a greater divergence than the science light in order to improve initial signal capture but otherwise are completely co-axial with the science light. The science light has a $1/e^2$ diameter of 4 cm but this is stopped down to 2.5 cm to improve light collection given the typical atmospheric coherence length close to the ground in Boulder.

At the receiver this path is reversed; the terminal collects the received light though the telescope and directs it off the galvanometric mirror. The received beacon is then de-multiplexed from the received science light and directed onto a quadrant detector, while the science light is coupled into single-mode, polarization maintaining fiber which is then connected to the heterodyne module. The dichroic mirror before the quadrant detector allows for the separation of the incoming and outgoing beacon lasers. The signals from the quadrant detector are fed into an analog feedback system that controls the *x-y* galvanometric mirror pair in order to center the beacon laser on the quad detector. With an appropriately aligned terminal, this will also maximize the science coupled into the single mode fiber. As a consequence of this feedback and the single-mode nature of the link, the outgoing light will be pre-aligned to the terminal at the distant end of the link.

A first generation set of terminals exhibited 3 dB of loss per terminal. A second generation set of terminals shows a loss of only 1.5 dB per terminal with the replacement of the parabolic reflecting telescope with a lensed telescope. The lensed telescope has a narrower spectral coverage but can still support light across the whole C-band. As the light passes through both terminals before detection reducing the insertion loss can greatly improve the dynamic range that can be supported.

The total power launched at the free-space optical terminal aperture is ~ 10 mW, comprising 2.5 mW of comb power, 2.5 mW of communication/coarse timing signal power, and 5 mW of beacon power. Figure 7 shows the spectrum of the launched light. The received comb power varies between 0 and 1 μW, depending on turbulence, and can suffer turbulence induced dropouts, i.e. the received power is below the detection threshold. The system is robust against such dropouts, however, as most turbulence-induced dropouts are less than 10 ms in duration[1].

6. VERIFICATION OF SYNCHRONIZATION

6.1 Methods of Synchronization Verification

As the 4 km link is folded back on itself via a distant mirror, a simple "out of loop" truth comparison is possible. As show in, a ~ 1m fiber path connects the remote and master sites. (Note that all in-loop signals traverse the 4 km air path.) The remote comb's carrier-envelope-offset frequency is purposefully offset relative to the master carrier-envelop-offset frequency by 1 MHz; 1 MHz is chosen for ease of demodulation. At the reference plane (red dashed line of Figure 10c), when the master and remote pulse trains overlap, we measure a 1 MHz heterodyne signal whose amplitude is proportional to the out-of-loop time offset. After an initial calibration step, this signal yields the time offset shown in Figure 14. As discussed below, temperature fluctuations of the ~ 1 m fiber path dominate the synchronization verification measurement on long timescales.

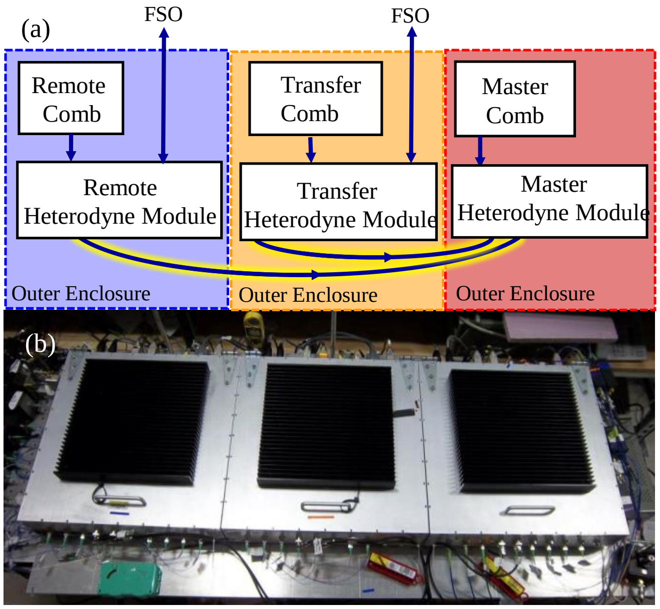


Figure 13. Co-located combs allow for synchronization verification with only a short out-of-loop fiber path. (a) Schematic of the three adjacent outer enclosures each containing a frequency comb and the associated heterodyne detection module. Critical fiber paths are highlight in yellow. Small holes allow the critical fibers to pass between adjacent outer enclosures. Blue lines indicate polarization-maintaining fiber. FSO: free-space optical terminal (b) Image of three adjacent outer enclosures.

An additional verification of the unambiguous synchronization of the two clocks can be performed through generation of an optical pulse-per-second (PPS) by selecting a single pulse on each site with a Mach-Zehnder modulator (MZM). Detection of the optical PPS can be performed with a fast photodetector and oscilloscope to verify that only one out of $2x10^8$ pulses is present. The arrival of the remote and master optical PPS signals at a common reference plane defined at the oscilloscope at the same time demonstrates that there are no 5-ns slips; however, the time resolution of this verification is lower as it is limited by either the fast photodetectors or the oscilloscope.

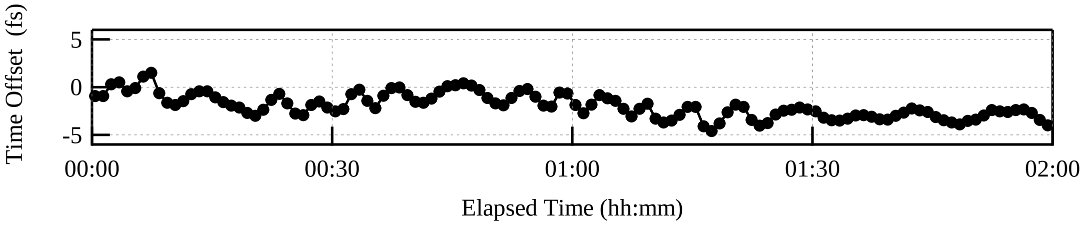


Figure 14. Example of out-of-loop measurement of time offset between master and remote clocks demonstrating femtosecond-level performance. Data has been down-sampled to 60 s so that the long timescale variation is more evident.

6.2 Impact of Temperature Fluctuations on Synchronization Verification

There are critical fiber paths which are not located within one of the temperature-controlled heterodyne modules, but pass between them. These paths are highlighted in yellow in Figure 13. The first of these fiber paths conveys the transfer comb to the master heterodyne module to measure their time offset, needed in the master synchronization equation. The second fiber path connects the outputs of the master and remote site for synchronization verification discussed in the previous section. (Note that this is the only connection of signals between the master and remote site that does not pass over the 4 km free-space link even though the two sites are adjacent in the laboratory.) Any temperature variations of these fiber paths will lead directly to time offset drifts in the synchronization verification.

To minimize this drift, the two fiber paths have been made as short as possible by placing the enclosures adjacent to each other with small holes drilled between them to pass the fibers. Each fiber path consists of ~ 1 m of polarization-maintaining fiber. The large enclosures are temperature controlled by water-cooled breadboards affixed to their top and bottom. As shown in Figure 15, we see a factor of 10 suppression of the external laboratory room temperature fluctuations within these enclosures. (The slight offsets between the three enclosures should be ignored as we use generic Steinhart-Hart coefficients[5] to compute the temperature rather than calibrating each thermistor.) The 1 °C peak-to-peak variations of Figure 15 would result in ~ 50 fs peak-to-peak variations in the delays for the 1 m fiber lengths. For Ref 1, the laboratory room temperature varied by 4 °C. Assuming the tenfold suppression within the enclosure, we would predict a 20 fs peak-to-peak variation. Instead, we observed a factor of two larger variation of 40 fs peak-to-peak, indicating additional contributions possibly from temperature gradients, additional out-of-loop fiber, temperature variations of the heterodyne modules, and the impacts of relative humidity and building vibration which are not accounted for here.

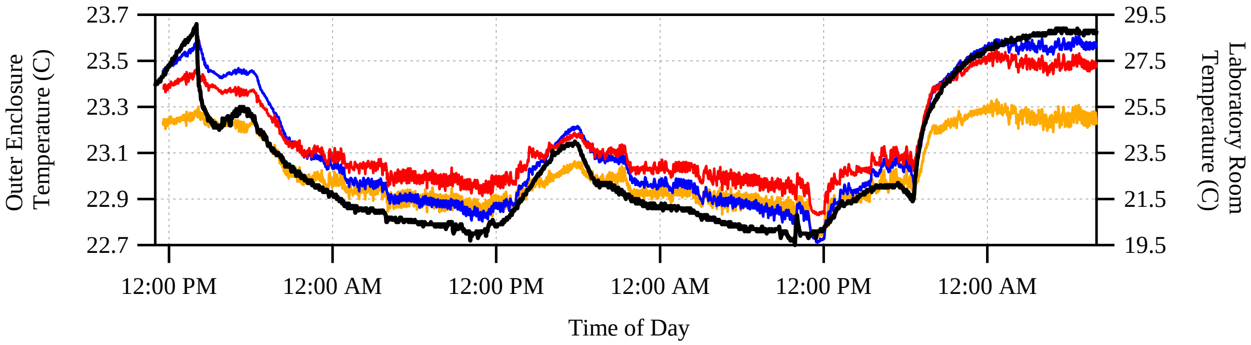


Figure 15. Suppression of laboratory room temperature fluctuations in outer enclosure. Over a two day period the laboratory showed a 10 °C variation in the room temperature (black trace). The three outer enclosures (red, blue, and orange) traces show only a 1 °C variation over the same period.

7. CONCLUSIONS

Here we have detailed the elements of the complex optical system needed to support femtosecond-level synchronization of clocks over turbulent air paths. While the system is not fully portable - in particular the optical cavities - there is no fundamental limitation to implementing a portable system based on the overall design shown here.

REFERENCES

[1] Deschenes, J.-D., Sinclair, L. C., Giorgetta, F. R., Swann, W. C., Baumann, E., Bergeron, H., Cermak, M., Coddington, I.., Newbury, N. R., “Synchronization of Distant Optical Clocks at the Femtosecond Level,” ArXiv150907888 Phys. (2015).

[2] Sinclair, L. C., Deschênes, J.-D., Sonderhouse, L., Swann, W. C., Khader, I. H., Baumann, E., Newbury, N. R.., Coddington, I., “Invited Article: A compact optically coherent fiber frequency comb,” Rev. Sci. Instrum. **86**(8), 081301 (2015).

[3] Shapiro, J. H., “Reciprocity of the Turbulent Atmosphere,” J Opt Soc Am **61**, 492–495 (1971).

[4] Coddington, I., Swann, W. C.., Newbury, N. R., “Coherent linear optical sampling at 15 bits of resolution,” Opt. Lett. **34**(14), 2153–2155 (2009).

[5] Steinhart, J. S.., Hart, S. R., “Calibration curves for thermistors,” Deep Sea Res. Oceanogr. Abstr. **15**(4), 497–503 (1968).

[6] Andrews, L. C.., Phillips, R. L., Laser beam propagation through random media, 2nd ed., SPIE, Bellingham, WA (2005).

Inferring the Stealthy Bridges between Enterprise Network Islands in Cloud Using Cross-Layer Bayesian Networks

Xiaoyan Sun[1], Jun Dai[1], Anoop Singhal[2], and Peng Liu[1]

[1] Penn State University, University Park, PA 16802, USA,
[2] National Institute of Standards and Technology, Gaithersburg, MD 20899, USA
{xzs5052,jqd5187}@ist.psu.edu, anoop.singhal@nist.gov, pliu@ist.psu.edu

Abstract. Enterprise networks are migrating to the public cloud to acquire computing resources for promising benefits in terms of efficiency, expense, and flexibility. Except for some public services, the enterprise network islands in cloud are expected to be absolutely isolated from each other. However, some "stealthy bridges" may be created to break such isolation due to two features of the public cloud: virtual machine image sharing and virtual machine co-residency. This paper proposes to use cross-layer Bayesian networks to infer the stealthy bridges existing between enterprise network islands. Prior to constructing cross-layer Bayesian networks, cloud-level attack graphs are built to capture the potential attacks enabled by stealthy bridges and reveal hidden possible attack paths. The result of the experiment justifies the cross-layer Bayesian network's capability of inferring the existence of stealthy bridges given supporting evidence from other intrusion steps in a multi-step attack.

Key words: cloud, stealthy bridge, Bayesian network, attack graph

1 Introduction

Enterprises have begun to move parts of their networks (such as web server, mail server, etc.) from traditional infrastructure into cloud computing environments. Cloud providers such as Amazon Elastic Compute Cloud (EC2) [1], Rackspace [2], and Microsoft's Azure cloud platform [3] provide virtual servers that can be rented on demand by users. This paradigm enables cloud customers to acquire computing resources with high efficiency, low cost, and great flexibility. However, it also introduces some security issues that are yet to be solved.

A public cloud can provide virtual infrastructures to many enterprises. Except for some public services, enterprise networks are expected to be like isolated islands in the cloud: connections from the outside network to the protected internal network should be prohibited. Consequently, an attack path that shows the multi-step exploitation sequence in an enterprise network should also be confined inside this island. However, as enterprise networks migrate into the cloud and replace traditional physical hosts with virtual machines, some "stealthy bridges" could be created between the isolated enterprise network islands, as shown in Fig. 1. Moreover, with the stealthy bridges, the attack path confined inside an enterprise network is able to traverse to another enterprise network in cloud.

Singhal, Anoop; Sun, Xiaoyan; Dai, Jun; Liu, Peng.
"Inferring the Stealthy Bridges between Enterprise Network Islands in Cloud Using Cross-Layer Bayesian Networks."
Paper presented at the 10th International Conference on Security and Privacy in Communication Networks, Beijing, China, Sep 24, 2014-Sep 26, 2014.

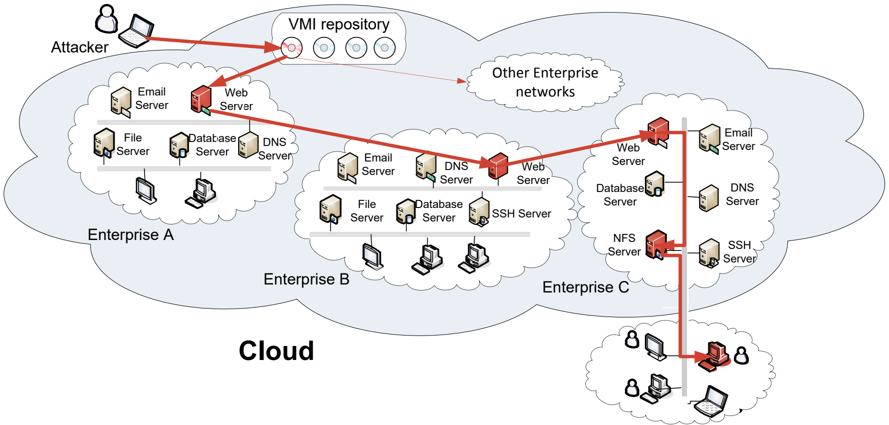


Fig. 1: The Attack Scenario

The creation of such “stealthy bridges” is enabled by two unique features of the public cloud. First, cloud users are allowed to create and share virtual machine images (VMIs) with other users. Besides, cloud providers also provide VMIs with pre-configured software, saving users’ efforts of installing the software from scratch. These VMIs provided by both cloud providers and users form a large repository. For convenience, users can take a VMI directly from the repository and instantiate it with ease. The instance virtual machine inherits all the security characteristics from the parent image, such as the security configurations and vulnerabilities. Therefore, if a user instantiates a *malicious* VMI, it’s like moving the attacker’s machine directly into the internal enterprise network, without triggering the Intrusion Detection Systems (IDSs) or the firewall. In this case, a “stealthy bridge” can be created via security holes such as backdoors. For example, in Amazon EC2, if an attacker intentionally leaves his public key unremoved when publishing an AMI (Amazon Machine Image), the attacker can later login into the running instances of this AMI with his own private key.

Second, virtual machines owned by different tenants may co-reside on the same physical host machine. To achieve high efficiency, customer workloads are multiplexed onto a single physical machine utilizing virtualization. Virtual machines on the same host may belong to unrelated users, or even rivals. Thus coresident virtual machines are expected to be absolutely isolated from each other. However, current virutalization mechanisms cannot ensure perfect isolation. The co-residency relationship can still enable security problems such as information leakage, performance interference [4], or even co-resident virtual machine crashing. Previous work [5] has shown that it is possible to identify on which physical host a target virtual machine is likely to reside, and then intentionally place an attacker virtual machine onto the same host in Amazon EC2. Once the coresidency is achieved, a “stealthy bridge” can be further established, such as a side-channel for passively observing the activities of the target machine to extract information for credential recovering [6], or a covert-channel for actively sending information from the target machine [8].

Stealthy bridges are stealthy information tunnels existing between disparate networks in cloud, that are unknown to security sensors and should have been forbidden. Stealthy bridges are developed mainly by exploiting *vulnerabilities that are unknown* to vulnerability scanners. Isolated enterprise network islands are connected via these stealthy tunnels, through which information (data, commands, etc.) can be acquired, transmitted or exchanged maliciously. Therefore stealthy bridges pose very severe threats to the security of public cloud. However, the stealthy bridges are inherently unknown or hard to detect: they either exploit unknown vulnerabilities, or cannot be easily distinguished from authorized activities by security sensors. For example, side-channel attacks extract information by passively observing the activities of resources shared by the attacker and the target virtual machine (e.g. CPU, cache), without interfering the normal running of the target virtual machine. Similarly, the activity of logging into an instance by leveraging intentionally left credentials (passwords, public keys, etc.) also hides in the authorized user activties.

The stealthy bridges can be used to construct a multi-step attack and facilitate subsequent intrusion steps across enterprise network islands in cloud. The stealthy bridges per se are difficult to detect, but the intrusion steps before and after the construction of stealthy bridges may trigger some abnormal activities. Human administrators or security sensors like IDS could notice such abnormal activities and raise corresponding alerts, which can be collected as the evidence of attack happening[1]. So our approach has two insights: 1) It is quite straightforward to build a cloud-level attack graph to capture the potential attacks enabled by stealthy bridges. 2) To leverage the evidence collected from other intrusion steps, we construct a cross-layer Bayesian Network (BN) to infer the existence of stealthy bridges. Based on the inference, security analysts will know where stealthy bridges are most likely to exist and need to be further scrutinized.

The main contributions of this paper are as follows:

First, a cloud-level attack graph is built by crafting new interaction rules in *MulVAL* [18], an attack graph generation tool. The cloud-level attack graph can capture the potential attacks enabled by stealthy bridges and reveal possible hidden attack paths that are previously missed by individual enterprise network attack graphs.

Second, based on the cloud-level attack graph, a cross-layer Bayesian network is constructed by identifying four types of uncertainties. The cross-layer Bayesian network is able to infer the existence of stealthy bridges given supporting evidence from other intrusion steps.

2 Cloud-level Attack Graph Model

A Bayesian network is a probabilistic graphical model that is applicable for real-time security analysis. Prior to the construction of a Bayesian Network, an attack graph should be built to reflect the attacks enabled by stealthy bridges.

[1] In our trust model, we assume cloud providers are fully trusted by cloud customers. In addition to security alerts generated at cloud level, such as alerts from hypervisors or cache monitors, the cloud providers also have the privilege of accessing alerts generated by customers' virtual machines.

2.1 Logical Attack Graph

An attack graph is a valuable tool for network vulnerability analysis. Current network defenders should not only understand how attackers could exploit a specific vulnerability to compromise one single host, but also clearly know how the security holes can be combined together for achieving an attack goal. An attack graph is powerful for dealing with the combination of security holes. Taking vulnerabilities existing in a network as the input, attack graph can generate the possible attack paths for a network. An attack path shows a sequence of potential exploitations to specific attack goals. For instance, an attacker may first exploit a vulnerability on Web Server to obtain the root privilege, and then further compromise Database Server through the acquired privilege. A variety of attack graphs have been developed for vulnerability analysis, mainly including state enumeration attack graphs [12, 13, 14] and dependency attack graphs [15, 16, 17]. The tool *MulVAL* employed in this paper is able to generate the logical attack graph, which is a type of dependency attack graph.

Fig. 2 shows part of an exemplar logical attack graph. There are two types of nodes in logical attack graph: derivation nodes (also called rule nodes, represented with ellipse), and fact nodes. The fact nodes could be further classified into primitive fact nodes (in rectangles), and derived fact nodes (in diamonds). Primitive fact nodes are typically objective conditions of the network, including network connectivity, host configuration, and vulnerability information. Derived fact nodes represent the facts inferred from logical derivation. Derivation nodes represent the interaction rules used for derivation. The directed edges in this graph represent the causality relationship between nodes. In a logical dependency attack graph, one or more fact nodes could serve as the preconditions of a derivation node and cause it to take effect. One or more derivation nodes could further cause a derived fact node to become true. Each derivation node represents the application of an interaction rule given in [19] that yields the derived fact.

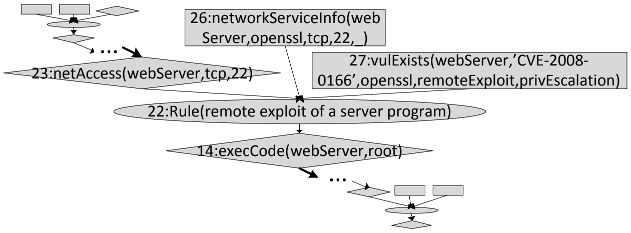

26:networkServiceInfo(web Server,openssl,tcp,22,_)
27:vulExists(webServer,'CVE-2008-0166',openssl,remoteExploit,privEscalation)
23:netAccess(webServer,tcp,22)
...
22:Rule(remote exploit of a server program)
14:execCode(webServer,root)
...

Fig. 2: A Portion of an Example Logical Attack Graph

For example, in Fig. 2, Node 26, 27 (primitive fact nodes) and Node 23 (derived fact node) are three fact nodes. They represent three preconditions respectively: Node 23, the attacker has access to the Web Server; Node 26, Web Server provides *OpenSSL* service; Node 27, Openssl has a vulnerability *CVE-2008-0166*. With the three preconditions satisfied simultaneously, the rule of Node 22 (derivation node) can take effect, meaning the remote exploit of a server program could happen. This derivation rule can further cause Node 14 (derived fact node) to be valid, meaning attacker can execute code on Web Server.

2.2 Cloud-level Attack Graph

In the cloud, each enterprise network can scan its own virtual machines for existing vulnerabilities and then generate an attack graph. The individual attack graph shows how attackers could exploit certain vulnerabilities and conduct a sequence of attack steps inside the enterprise network. However, such individual attack graphs are confined to the enterprise networks without considering the potential threats from cloud environment. The existence of stealthy bridges could activate the prerequisites of some attacks that are previously impossible in traditional network environment and thus enable new attack paths. These attack paths are easily missed by individual attack graphs. For example, in Fig. 1, without assuming the stealthy bridge existing between enterprise A and B, the individual attack graph for enterprise B can be incomplete or even not established due to lack of exploitable vulnerabilities. Therefore, a cloud-level attack graph needs to be built to incorporate the existence of stealthy bridges in the cloud. By considering the attack preconditions enabled by stealthy bridges, the cloud-level attack graph can reveal hidden potential attack paths that are missed by individual attack graphs.

The cloud-level attack graph should be modeled based on the cloud structure. Due to the VMI sharing feature and the co-residency feature of cloud, a public cloud has the following structural characteristics. First, virtual machines can be created by instantiating VMIs. Therefore virtual machines residing on different hosts may actually be instances of the same VMI. In simple words, they could have the same VMI parents. Second, virtual machines belong to one enterprise network may be assigned to a number of different physical hosts that are shared by other enterprise networks. That is, the virtual machines employed by different enterprise networks are likely to reside on the same host. As shown in Fig. 3, the vm_{11} on host 1 and vm_{2j} on host 2 may be instances of the same VMI, while vm_{12} and vm_{2k} could belong to the same enterprise network. Third, the real enterprise network could be a hybrid of a cloud network and a traditional network. For example, the servers of an enterprise network could be implemented in the cloud, while the personal computers and workstations could be in the traditional network infrastructure.

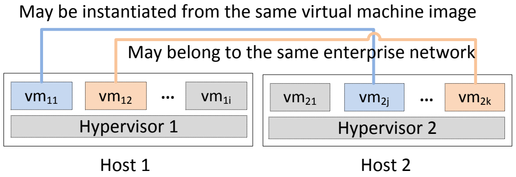

May be instantiated from the same virtual machine image
May belong to the same enterprise network
vm11
vm12
...
vm1i
Hypervisor 1
vm21
vm2j
...
vm2k
Hypervisor 2
Host 1
Host 2

Fig. 3: Features of the Public Cloud Structure

Due to the above characteristics of cloud structure, the model for the cloud-level attack graph should have the following corresponding characteristics.

1) The cloud-level attack graph is a cross-layer graph that is composed of three layers: virtual machine layer, VMI layer, and host layer, as shown in Fig. 4.

2) The virtual machine layer is the major layer in the attack graph stack. This layer reflects the causality relationship between vulnerabilities existing inside the virtual machines and the potential exploits towards these vulnerabilities. If

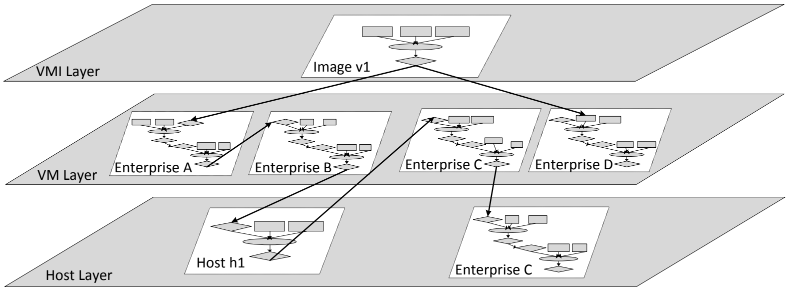


Fig. 4: An Example Cloud-level Attack Graph Model

stealthy bridges do not exist, the attack graph generated in this layer is scattered: each enterprise network has an individual attack graph that is isolated from others. The individual attack graphs can be the same as the ones generated by cloud customers themselves through scanning the virtual machines for known vulnerabilities. However, if stealthy bridges exist on the other two layers, the isolated attack graph could be connected, or even experience dramatic changes: some hidden potential attack paths will be revealed and the original attack graph is enriched. For example, in Fig. 4, without the stealthy bridge on *h1*, attack paths in enterprise network C will be missing or incomplete because no exploitable vulnerability is available as the entry point for attack.

3) The VMI layer mainly captures the stealthy bridges and corresponding attacks caused by VMI sharing. Since virtual machines in different enterprise networks may be instantiated from the same parent VMI, they could inherit the same security issues from parent image, such as software vulnerabilities, malware, or backdoors, etc. Evidence from [20] shows that 98% of Windows VMI and 58% of Linux VMIs in Amazon EC2 contain software with critical vulnerabilities. A large number of software on these VMIs are more than two years old. Since cloud customers take full responsibility for securing their virtual machines, many of these vulnerabilities remain unpatched and thus pose great risks to cloud. Once a vulnerability or an attack type is identified in the parent VMI, the attack graph for all the children virtual machine instances may be affected: a precondition node could be activated, or a new interaction rule should be constructed in attack graph generation tool.

The incorporation of the VMI layer provides another benefit to the subsequent Bayesian network analysis. It enables the interaction between the virtual machine layer and the VMI layer. On one hand, the probability of a vulnerability existence on a VMI will affect the probability of the vulnerability existence on its children instance virtual machines. On the other hand, if new evidence is found regarding the vulnerability existence on the children instances, the probability change will in turn influence the parent VMI. If the same evidence is observed on multiple instances of the VMI, this VMI is very likely to be problematic.

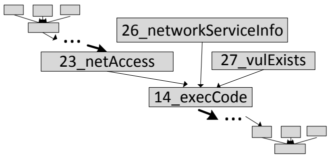
4) The host layer is able to reason exploits of stealthy bridges caused by virtual machine co-residency. Exploits on this layer could lead to further penetrations on the virtual machine layer. In addition, this layer actually captures all attacks that could happen on the host level, including those on pure physical

Singhal, Anoop; Sun, Xiaoyan; Dai, Jun; Liu, Peng.
"Inferring the Stealthy Bridges between Enterprise Network Islands in Cloud Using Cross-Layer Bayesian Networks."
Paper presented at the 10th International Conference on Security and Privacy in Communication Networks, Beijing, China, Sep 24, 2014-Sep 26, 2014.

hosts with no virtual machines. Hence it provides a good interface to hybrid enterprise networks that are implemented with partial cloud and partial traditional infrastructures. The potential attack paths identified on the cloud part could possibly extend to traditional infrastructures if all prerequisites for the remote exploits are satisfied, such as network access being allowed, and exploitable vulnerabilities existing, etc. As in Fig. 4, the attack graph for enterprise C extends from virtual machine layer to host layer.

3 Cross-layer Bayesian Networks

A Bayesian network (BN) is a probabilistic graphical model representing cause and effect relations. For example, it is able to show the probabilistic causal relationships between a disease and the corresponding symptoms. Formally, a Bayesian network is a Directed Acyclic Graph (DAG) that contains a set of nodes and directed edges. The nodes represent random variables of interest and the directed edges represent the causal influence among the variables. The strength of such influence is represented with a conditional probability table (CPT). For example, Fig. 5 shows a portion of a BN constructed directly from the attack graph in Fig. 2 by removing the rule Node 22. Node 14 can be associated with the CPT table as shown. This CPT means that if all of the preconditions of Node 14 are satisfied, the probability of Node 14 being true is 0.9. Node 14 is false in all other cases.



26	27	23	14
T	T	T	0.9
otherwise			0

Fig. 5: A Portion of Bayesian Network with associated CPT table

A Bayesian network can be used to compute the probabilities of variables of interest. It is especially powerful for diagnosis and prediction analysis. For example, in diagnosis analysis, given the symptoms being observed, a BN can calculate the probability of the causing fact (respresented with $\Pr(cause \mid symptom = True)$). While in prediction analysis, given the causing fact, a BN will predict the probability of the corresponding symptoms showing up ($Pr(symptom|cause = True)$). In the cybersecurity field, similar diagnosis and prediction analysis can also be performed, such as calculating the probability of an exploitation happening if related IDS alerts are observed($Pr(exploitation|IDSalert = True)$), or the probability of the IDS raising an alert if an exploitation already happened ($Pr(IDSalert|exploitation = True)$). This paper mainly carries out a diagnosis analysis that computes the probability of stealthy bridge existence by collecting evidence from other intrusion steps. Diagnosis analysis is a kind of "backward" computation. In the cause-and-symptom model, a concrete evidence about the symptom could change the posterior probability of the cause by computing $Pr(cause|symptom = True)$. More intuitively, as more evidence is collected regarding the symptom, the probability of the cause will become closer to reality if the BN is constructed properly.

3.1 Identify the Uncertainties

Inferring the existence of stealthy bridges requires real-time evidence being collected and analyzed. BN has the capability, which attack graphs lack, of performing such real-time security analysis. Attack graphs correlate vulnerabilities and potential exploits in different machines and enables *determinstic* reasoning. For example, if all the preconditions of an attack are satisfied, the attacker *should* be able to launch the attack. However, in *real-time* security analysis, there are a range of uncertainties associated with this attack that cannot be reflected in an attack graph. For example, has the attacker chosen to launch the attack? If he launched it, did he succeed to compromise the host? Are the Snort [22] alerts raised on this host related to the attack? Should we be more confident if we got other alerts from other hosts in this network? Such uncertainty aspects should be taken into account when performing real-time security analysis. BN is a valuable tool for capturing these uncertainties.

One non-trivial difficulty for constructing a well functioning BN is to identify and model the uncertainty types existing in the attack procedure. In this paper, we mainly consider four types of uncertainties related to cloud security.

Uncertainty of stealthy bridges existence. The presence of known vulnerabilities is usually deterministic due to the availability of vulnerability scanners. After scanning a virtual machine or a physical host, the vulnerability scanner such as Nessus [24] is able to tell whether a known vulnerability exists or not[2]. However, due to its unknown or hard-to-detect feature, effective scanners for stealthy bridges are rare. Therefore, the existence of stealthy bridges itself is a type of uncertainty. In this paper, to enable the construction of a complete attack graph, stealthy bridges are hypothesized to be existing when corresponding conditions are met. For example, if two virtual machines co-reside on the same physical host and one of them has been compromised by the attacker, the attack graph will be generated by making a hypothesis that a stealthy bridge can be created between these two virtual machines. This is enforced by crafting a new interaction rule as follows in *MulVAL*:

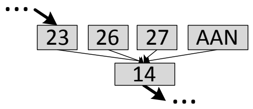
```
interaction rule(
   (stealthyBridgeExists(Vm_1,Vm_2, Host, stealthyBridge_id):-
      execCode(Vm_1,_user),
      ResideOn(Vm_1, Host),
      ResideOn(Vm_2, Host)),
  rule_desc('A stealthy bridge could be built between virtual machines co-residing on
 the same host after one virtual machine is compromised')).
```

Afterwards, the BN constructed based on the attack graph will infer the probability of this hypothesis being true.

Uncertainty of attacker action. Uncertainty of attacker action is first identified by [23]. Even if all the prerequsites for an attack are satisfied, the attack may not happen because attackers may not take action. Therefore, a kind of Attack Action Node (AAN) is added to the BN to model attackers' actions. An AAN node is introduced as an additional parent node for the attack. For example, the BN shown in Fig. 5 is changed to Fig. 6 after adding an AAN node.

[2] The assumption here is that a capable vulnerability scanner is able to scan out all the known vulnerabilities.

Correspondingly, the CPT table is modified as in Fig. 6. This means “attacker taking action” is another prerequisite to be satisfied for the attack to happen.



26 27 23 AAN	14
T T T T	0.9
otherwise	0

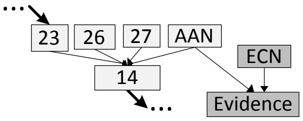
Fig. 6: A Portion of Bayesian Network with AAN node

An AAN node is not added for all attacks. They are needed only for important attacks such as the very first intrusion steps in a multi-step attack, or attacks that need attackers’ action. Since an AAN node represents the primitive fact of whether an attacker taking action and has no parent nodes, a prior probability distribution should be assigned to an AAN to indicate the likelihood of an attack. The posterior probability of AAN will change as more evidence is collected.

Uncertainty of exploitation success. Uncertainty of exploitation success goes to the question of “did the attacker succeed in this step?”. Even if all the prerequisites are satisfied and the attacker indeed launches the attack, the attack is not guarenteed to succeed. The success likelihood of an attack mainly depends on the exploit difficulty of vulnerabilities. For some vulnerabilities, usable exploit code is already publicly available. While for some other vulnerabilities, the exploit is still in the proof-of-concept stage and no successful exploit has been demonstrated. Therefore, the exploit difficulty of a vulnerability can be used to derive the CPT table of an exploitation. For example, if the exploit difficulty for the vulnerability in Fig. 5 is very high, the probability for Node 14 when all parent nodes are true could be assigned as very low, such as 0.3. If in the future a public exploit code is made available for this vulnerability, the probability for Node 14 may be changed to a higher value accordingly. The National Vulnerability Database (NVD) [25] maintains a CVSS [26] scoring system for all CVE [27] vulnerabilities. In CVSS, Access Complexity (AC) is a metric that describes the exploit complexity of a vulnerability using values of “high”, “medium”, “low”. Hence the AC metric can be employed to derive CPT tables of exploitations and model the uncertainty of exploitation success.

Uncertainty of evidence. Evidence is the key factor for BN to function. In BN, uncertainties are indicated with probability of related nodes. Each node describes a real or hypothetical event, such as “attacker can execute code on Web Server”, or “a stealthy bridge exists between virtual machine A and B”, etc. *Evidence is collected to reduce uncertainty* and calculate the probabilities of these events. According to the uncertainty types mentioned above, evidence is also classified into three types: evidence for stealthy bridges existence, evidence for attacker action, and evidence for exploitation success. Therefore, whenever a piece of evidence is observed, it is assigned to one of the above evidence types to support the corresponding event. This is done by adding evidence as the children nodes to the event nodes related to uncertainty. For example, an IDS alert about a large number of login attempts can be regarded as evidence of attacker action, showing that an attacker could have tried to launch an attack. This evidence is then added as the child node to an AAN, as exemplified in Fig. 7. For another example, the alert “system log is deleted” given by Tripwire [28] can be the child of the node “attacker can execute code”, showing that an exploit has been successfully achieved.

However, evidence per se contain uncertainty. The uncertainty is twofold. First, the support of evidence to an event is uncertain. For analogy, a symptom of coughing cannot completely prove the presence of lung disease. In the above examples, could the multiple login attempts testify that attackers have launched the attack? How likely is it that attackers have succeeded in compromising the host if a system log deletion is observed? Second, evidence from security sensors is not 100% accurate. IDS systems such as Snort, Tripwire, etc. suffer a lot from a high false alert rate. For example, an event may trigger an IDS to raise an alert while actually no attack happens. In this case, the alert is a false positive. The reverse case is a false negative, that is, when an IDS should have raised an alarm but doesn’t. Therefore, we propose to model the uncertainty of evidence with an Evidence-Confidence(EC) pair as shown in Fig. 7. The EC pair has two nodes, an Evidence node and an Evidence Confidence Node (ECN). An ECN is assigned as the parent of an Evidence node to model the confidence level of the evidence. If the confidence level is high, the child evidence node will have larger impact on other nodes. Otherwise, the evidence will have lower impact on others. An example CPT associated with the evidence node is given in Fig. 7. Whenever new evidence is observed, an EC pair is attached to the supported node. A node can have several EC pairs attached with it if multiple instances of evidence are observed. With ECN nodes, security experts can tune confidence levels of evidence with ease based on their domain knowledge and experience. This will greatly enhance the flexibility and accuracy of BN analysis.



AAN	True					False				
ECN	VeryHigh	High	Medium	Low	None	VeryHigh	High	Medium	Low	None
True	0.95	0.8	0.6	0.55	0.5	0.05	0.2	0.4	0.45	0.5
False	0.05	0.2	0.4	0.45	0.5	0.95	0.8	0.6	0.55	0.5

Fig. 7: The Evidence-Condidence Pair and Associated Exemplar CPT

4 Implementation

4.1 Cloud-level Attack Graph Generation

This paper uses *MulVAL* [19] as the attack graph generation tool. To construct a cloud-level attack graph, new primitive fact nodes and interaction rules have to be crafted in *MulVAL* on the VMI layer and host layer to model the existence of stealthy bridges. Each virtual machine has an ID tuple *(Vm_id, VMI_id, H_id)* associated with it, which represents the ID for the virtual machine itself, the VMI it was derived from, and the host it resides on. The VMI layer mainly focuses on the model of VMI vulnerability inheritance and the VMI backdoor problems. The host layer mainly focuses on modeling the virtual machine co-residency problems. Table 1 provides a sample set of newly crafted interaction rules that are incorporated into *MulVAL* for cloud-level attack graph generation.

4.2 Construction of Bayesian Networks

Deriving Bayesian networks from cross-layer attack graphs consists of four major components: removing rule nodes in the attack graph, adding new nodes, determining prior probabilities, and constructing CPT tables.

Table 1: a Sample Set of Interaction Rules

```
/***Model the Virtual Machine Image Vulnerability Inheritance***/
primitive(IsInstance(Vm_id, VMI_id))
primitive(ImageVulExists(VMI_id, vulID, _program, _range, _consequence))
derived(VulExists(Vm_id, vulID, _program,_range,_consequence)).

%remove vulExists from the primitive fact set
primitive(vulExists(_host, _vulID, _program, _range, _consequence)

interaction rule(
   (VulExists(Vm_id, vulID, _program, _range, _consequence):-
      ImageVulExists(VMI_id, vulID, _program, _range, _consequence),
      IsInstance(Vm_id, VMI_id)),
    rule_desc(‘A virtual machine instance inherits the vulnerability from the parent VMI’)).

/***Model the Virtual Machine Image Backdoor Problem***/
primitive(IsThirdPartyImage(VMI_id)).
derived(ImageVulExists(VMI_id, sealthyBridge_id, _, _remoteExploit, privEscalation)).

interaction rule(
   (ImageVulExists(VMI_id,stealthyBridge_id, _, _remoteExploit, privEscalation):-
      IsThirdPartyImage(VMI_id)),
    rule_desc(‘A third party VMI could contain a stealthy bridge’)).

interaction rule(
   (execCode(Vm_id, Perm):
      VulEixsts(Vm_id, stealthyBridge_id, _, _, privEscalation),
      netAccess(H, _Protocol, _Port)),
    rule_desc(‘remoteExploit of a stealthy bridge’)).

/***Model the Virtual Machine Co-residency Problem***/
primitive(ResideOn(VM_id, H_id)).
derived(stealthyBridgeExists(Vm_1,Vm_2, H_id, stealthyBridge_id).

interaction rule(
   (stealthyBridgeExists(Vm_1,Vm_2, Host, stealthyBridge_id):-
      execCode(Vm_1,_user),
      ResideOn(Vm_1, Host),
      ResideOn(Vm_2, Host)),
   rule_desc(‘A stealthy bridge could be built between virtual machines co-residing on
 the same host after one virtual machine is compromised’)).

interaction rule(
   (execCode(Vm_2,_user):-
      stealthyBridgeExists(Vm_1,Vm_2, Host, stealthyBridge_id)),
    rule_desc(‘A stealthy bridge could lead to privilege escalation on victim machine’)).

interaction rule(
   (canAccessHost(Vm_2):-
      logInService(Vm_2,Protocol,Port),
      stealthyBridgeExists(Vm_1,Vm_2,Host,stealthyBridge_id)),
    rule_desc(‘Access a host through a log-in service by obtaining authentication
information through stealthy bridges’)).
```

Remove rule nodes of attack graph. In an attack graph, the rule nodes imply how postconditions are derived from preconditions. The derivation is deterministic and contains no uncertainty. Therefore, these rule nodes have no effect on the reasoning process, and thus can be removed when constructing the BN. To remove a rule node, its preconditions are connected directly to its postconditions. For example, in Fig. 2, Node 26, 27, and 23 will be connected directly to Node 14 by removing Node 22.

Adding new nodes. New nodes are added to capture the uncertainty of attacker action and the uncertainty of evidence. To capture the uncertainty of attacker action, each step has a separate AAN node as the parent, rather than sharing the same AAN among multiple steps. The AAN node models attacker action at the granularity of attack steps, and thus reflects the actual attack paths. To model the uncertainty of evidence, whenever new evidence is observed, an EC pair is constructed and attached to the supported node with uncertainty.

Determining prior probabilities. Prior probability distributions should be determined for all root nodes that have no parents, such as the vulnerability existence nodes, the network access nodes, or the AAN nodes.

Constructing CPT tables. Some CPT tables can be determined according to a standard, such as the the AC metric in CVSS scoring system. The AC metric describes the exploit complexity of vulnerabilities and thus can be used to derive the CPT tables for corresponding exploitations. Some other CPT tables may involve security experts' domain knowledge and experience. For example, the VMIs from a trusted third party may have lower probability of containing security holes such as backdoors, while those created and shared by individual cloud users may have higher probability.

The constructed BN should be robust against small changes in prior probabilities and CPT tables. To ensure such robustness, we use *SamIam* [33] for sensitivity analysis when constructing and debugging the BN. By specifying the requirements for an interested node's probability, *SamIam* will check the associated CPT tables and provide suggestions on feasible changes. For example, if we want to change $P(N5 = True)$ from 0.34 to 0.2, *SamIam* will provide two suggestions, either changing $P(N5 = True|N2 = True, N3 = True)$ from 0.9 to <= 0.43, or changing $P(N3 = True|N1 = True)$ from 0.3 to <= 0.125.

5 Experiment

5.1 Attack Scenario

Fig. 1 shows the network structure in our attack scenario. We have 3 major enterprise networks: A, B, and C. A and B are all implemented within the cloud, while C is implemented by partially cloud, and partially traditional network (the servers are located in the cloud and the workstations are in a traditional network). The attack includes several steps conducted by attacker Mallory.

Step 1, Mallory first publishes a VMI that provides a web service in the cloud. This VMI is malicious in that it contains a security hole that Mallory knows how to exploit. For example, this security hole could be an SSH user authentication key (the public key located in *.ssh/authorized_keys*) that is intentionally left in the VMI by Mallory. The leftover creates a backdoor that allows Mallory to login into any instances derived from this malicious VMI using his own private key. The security hole could also be an unknown vulnerability that is not yet publicly known. To make the attack scenario more generic, we choose a vulnerability *CVE-2007-2446* [29], existing in *Samba 3.0.0* [30], as the one imbedded in the malicious VMI, but assume it as *unknown* for the purpose of simulation.

Step 2, the malicious VMI is then adopted and instantiated as a web server by an innocent user from A. Mallory now wants to compromise the live instances, but he needs to know which instances are derived from his malicious VMI. [20] provides three possible ways for machine fingerprinting: ssh matching, service matching, and web matching. Through ssh key matching, Mallory finds the right instance in A and completes the exploitation towards *CVE-2007-2446* [29].

Step 3, enterprise network B provides web services to a limited number of customers, including A. With the acquired root privilege from A's web server, Mallory is able to access B's web server, exploit one of its vulnerabilities *CVE-2007-5423* [31] from application *tikiwiki 1.9.8* [32], and create a reverse shell.

Step 4, Mallory notices that enterprise B and C has a special relationship: their web servers are implemented with virtual machines co-residing on the same host. C is a start-up company that has some valuable information stored on its CEO's workstation. Mallory then leverages the co-residency relationship of the web servers and launches a side-channel attack towards C's web server to extract its password. Mallory obtains user privilege through the attack. Mallory also establishes a covert channel between the co-resident virtual machines for convenient information exchange.

Step 5, the NFS server in C has a directory that is shared by all the servers and workstations inside the company. Normally C's web server should not have *write* permission to this shared directory. But due to a configuration error of the NFS export table, the web server is given *write* permission. Therefore, if Mallory can upload a Trojan horse to the shared directory, other innocent users may download the Trojan horse from this directory and install it. Hence Mallory crafts a Trojan horse *management_tool.deb* and uploads it into the shared NSF directory on web server.

Step 6, The innocent CEO from C downloads *management_tool.deb* and installs it. Mallory then exploits the Trojan horse and creats a unsolicited connection back to his own machine.

Step 7, Mallory's VMI is also adopted by several other enterprise networks, so Mallory compromises their instances using the same method in Step 2.

In this scenario, two stealthy bridges are established[3]: one is from Internet to enterprise network A through exploiting an unknown vulnerability, the other one is between enterprise network B and C by leveraging virtual machine co-residency. The attack path crosses over three enterprise networks that reside in the same cloud, and extends to C's traditional network.

5.2 Experiment Result

The purpose of our experiment is to check whether the BN-based tool is able to infer the existence of stealthy bridges given the evidence. The Bayesian network has two inputs: the network deployment (network connection, host configuration, and vulnerability information, etc.) and the evidence. The output of BN is the probability of specific events, such as the probability of stealthy bridges being established, or the probability of a web server being compromised. We view the attackers' sequence of attack steps as a set of ground truth. To evaluate the effectiveness of the constructed BN, we compare the output of the BN with the ground truth of the attack sequence. For example, given the ground truth that a

[3] The enterprise networks in Step 7 are not key players, so we do not analyze the stealthy bridges established in this step, but still use the raised alerts as evidence.

stealthy bridge has been established, we will check the corresponding probability provided by the BN to see whether the result is convincible.

For the attack scenario illustrated in Fig. 1, the cross-layer BN is constructed as in Fig. 8. By taking into account the existence of stealthy bridges, the cloud-level attack graph has the capability of revealing potential hidden attack paths. Therefore, the constructed BN also inherits the revealed hidden paths from the cloud-level attack graph. For example, the white part in Fig. 8 shows the hidden paths enabled by the stealthy bridge between enterprise network B and C. These paths will be missed by individual attack graphs if the stealthy bridge is not considered. The inputs for this BN are respectively the network deployment shown in Table 2[4] and the collected evidence is shown in Table 3. Evidence is collected against the attack steps described in our attack scenario. Not all attack steps have corresponding observed evidence.

Table 2: Network Deployment

Node	Deployed Facts
N1	IsThirdPartyImage(VMI)
N2	IsInstance(Aws, VMI)
N4	netAccess(Aws,_protocol,_port)
N17	netServiceInfo(Bws,tikiwiki,http,80,_)
N19	ResideOn(Bws,H)
N20	ResideOn(Cws,H)
N21	hacl(Cws,Cnfs,nfsProtocol,nfsPort)
N27	nfsExport(Cnfs,'/export',write,Cws)
N30	nfsMountd(CworkStation,'/mnt/share', Cnfs,'/export',read)
N32	VulExists(CworkStation,'CVE-2009-2692',kernel,localExploit,privEscalation)
N41	IsInstance(Dws,VMI)
N43	netAccess(Dws,_protocol,_port)

Table 3: Collected Evidence Corresponding to Attack Steps

Node	Step	Collected Evidence
N9	2	Wireshark shows multiple suspicious connections established
N11	2	IDS shows malicious packet detected
N13	2	Wireshark "follow tcp stream" shows a back telnet connection is instructed to open
N23	4	Cache monitor observes abnormal cache activities
N34	5	Tripwire shows several file modification toward management_tool.deb
N37	6	IDS shows Trojan horse installation
N39	6	Wireshark "follow tcp stream" find plain text in supposed encrypted-connection
N47	7	Wireshark shows a back telnet connection is instructed to open
N49	7	IDS shows malicious packet detected

We conducted four sets of simulation experiments, each with a specific purpose. For simplicity, we assume all attack steps are completed instantly with no time delay. The ground truth in our attack scenario tells that one stealthy bridge between attacker and enterprise A is established in attack step 2, and the other one between B and C is established in step 4. By taking evidence with a certain order as input, the BN will generate a corresponding sequence of probabilities for events of interest. The probabilities are compared with the ground truth to evaluate the performance of the BN.

In experiment 1, we assume all the evidence is observed in the order of the corresponding attack steps. We are interested in four events, a stealthy bridge exists in enterprise A's web server (N5), the attacker can execute arbitrary code

[4] Aws,Bws,Cws,Cnfs,Cworkstation denote A's web server, B's web server, C's web server, C's NFS server, C's workstation respectively.

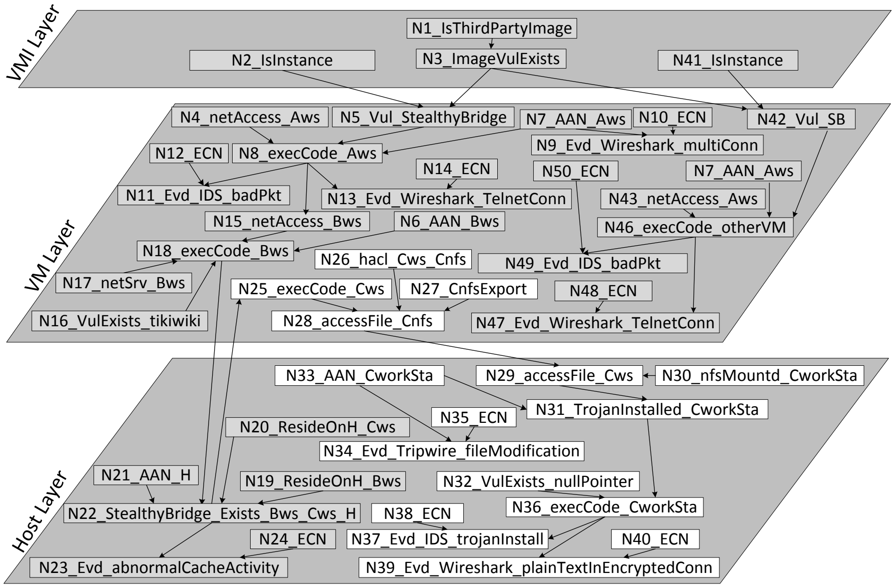


Fig. 8: The Cross-Layer Bayesian Network Constructed for the Attack Scenario

on A's web server (N8), a stealthy bridge exists in the host that B's web server reside (N22), and the attacker can execute arbitrary code on C's web server (N25). N8 and N25 respectively imply that the stealthy bridges in N5 and N22 are successfully established. Table 4 shows the results of experiment 1 given supporting evidence with corresponding confidence values. The results indicate that the probability of stealthy bridge existence is initially very low, and increases as more evidence is collected. For example, $Pr(N5 = True)$ increases from 34% with no evidence observed to 88.95% given all evidence presented. This means that a stealthy bridge is very likely to exist on enterprise A's web server after enough evidence is collected.

The first stealthy bridge in our attack scenario is established in attack step 2, and the corresponding pieces of evidence are N9, N11, and N13. $Pr(N8 = True)$ is 95.77% after all the evidence from step 2 is observed, but $Pr(N5 = True)$ is only 74.64%. This means that although the BN is almost sure that A's web server has been compromised, it doesn't have the same confidence of attributing the exploitation to the stealthy bridge, which is caused by the unknown vulnerability inherited from a VMI. $Pr(N5 = True)$ increases to 88.95% only after evidence N47 and N49 from other enterprise networks is observed for attack step 7. This means that if the same alerts appear in other instances of the same VMI, the VMI is very likely to contain the related unknown vulnerability.

The second stealthy bridge is established in step 4, and the corresponding evidence is N23. $Pr(N22 = True)$ is 57.45% after evidence N9 to N23 is collected. The number seems to be low. However, considering the unusual difficulty of leveraging a co-residency relationship, this low probability still should be treated with great attention. After all evidence is observed, the increase of $Pr(N22 =$

$True$) from 13.91% to 73.29% may require security experts to carefully scrutinize the virtual machine isolation status on the related host.

Table 4: Results of Experiment 1

Events	No evidence	N9 Medium	N11 High	N13 High	N23 High	N34 VeryHigh	N37 High	N39 VeryHigh	N47 VeryHigh	N49 VeryHigh
N5=True	34%	34%	51.54%	74.64%	75.22%	75.22%	75.41%	75.5%	86.07%	88.95%
N8=True	20.25%	22.96%	54.38%	95.77%	96.81%	96.81%	97.14%	97.31%	98.14%	98.37%
N22=True	13.91%	14.32%	19.03%	25.23%	57.45%	57.45%	67.67%	73.04%	73.24%	73.29%
N25=True	17.52%	17.89%	22.13%	27.71%	56.7%	56.7%	68.11%	74.1%	74.27%	74.32%

Experiment 2 tests the influence of false alerts to BN. In this experiment, we assume evidence N11 is a false alert generated by IDS. We perform the same analysis as in experiment 1 and compare results with it. Table 5 shows that when only 3 pieces of evidence (N9, N11, and N13) are observed, the probability of the related event is greatly affected by the false alert. For instance, $Pr(N5 = True)$ is 74.64% when N11 is correct, and is 53.9% when N11 is a false alert. But $Pr(N8 = True)$ is not greatly influenced by N11 because it's not closely related to the false alert. When all evidence is input into the BN, the influence of false alerts to related events is reduced to an acceptable level. This shows that a BN can provide relatively correct answer by combining the overall evidence set.

Table 5: Results of Experiment 2

Events	with 3 pieces of evidence		with all evidence	
	N11=True	N11=False	N11=True	N11=False
N5	74.64%	53.9%	88.95%	79.59%
N8	95.77%	58.6%	98.37%	79.07%
N22	25.23%	19.66%	73.29%	68.62%
N25	27.71%	22.7%	74.32%	70.24%

Since security experts may change their confidence value towards evidence based on their new knowledge and observation, experiment 3 tests the influence of evidence confidence value to the BN. This experiment generates similar results as in experiment 2, as shown in Table 6. When evidence is rare, the confidence value changes from VeryHigh to Low has larger influence to related events than when evidence is sufficient.

Table 6: Results of Experiment 3

Events	with 3 pieces of evidence		with all evidence	
	N14=VeryHigh	N14=Low	N14=VeryHigh	N14=Low
N5	74.64%	54.29%	88.95%	79.82%
N8	95.77%	59.30%	98.37%	79.54%
N22	25.23%	19.77%	73.29%	68.73%
N25	27.71%	22.79%	74.32%	70.34%

In experiment 4, we test the affect of evidence input order to the BN analysis result. We bring forward the evidence N47 and N49 from step 7 and insert them before N23 and N37 respectively. The analysis shows that a BN can still produce reliable results in the presence of changing evidence order.

6 Related Work

We explore the literature for the following topics that are related to our paper.

VMI sharing. [34] explores a variety of attacks that leverage the virtual machine image sharing in Amazon EC2. Researchers were able to extract highly sensitive information from publicly available VMIs. The analysis revealed that 30% of the 1100 analyzed AMIs (Amazon Machine Images) at the time of the

SP-942
Singhal, Anoop; Sun, Xiaoyan; Dai, Jun; Liu, Peng.
"Inferring the Stealthy Bridges between Enterprise Network Islands in Cloud Using Cross-Layer Bayesian Networks."
Paper presented at the 10th International Conference on Security and Privacy in Communication Networks, Beijing, China, Sep 24, 2014-Sep 26, 2014.

analysis contained public keys that are backdoors for the AMI Publishers. The backdoor problem is not limited to AMIs created by individuals, but also affects those from well-known open-source projects and companies.

Co-Residency. The security issues caused by virtual machine co-residency have attracted researchers' attention recently. [11] pointed out that the shared resource environment of cloud will introduce security issues that are fundamentally new and unique to cloud. [5] shows how attackers can identify on which host a target virtual machine is likely to reside in Amazon EC2, and then place the malicious virtual machine onto the same host through a number of instantiating attemps. Such co-residency can be used for further malicious activities, such as launching side-channel attack to extract information from a target virtual machine [6]. [10] takes an opposite perspective and proposes to detect co-residency via side-channel analysis. [4] demonstrates a new class of attacks called resource-freeing attacks (RFAs), which leverage the performance interference of co-resident virtual machine. [8] presents a traffic analysis attack that can initiate a covert channel and confirm co-residency with a target virtual machine instance. [7] also considers attacks towards hypervisor and propose to eliminate the hypervisor attack surface through new system design.

Bayesian Networks. BNs have been applied to intrusion detection [35] and cyber security analysis in traditional networks [23]. [23] analyzes which hosts are likely to be compromised based on known vulnerabilities and observed alerts. Our work lands on a different cloud environment and takes a reverse strategy by using BN to infer the stealthy bridges, which are unknown in nature. In the future, the inference of stealthy bridges can be further extended to identify the zero-day attack paths in cloud, as in [9] for traditional networks.

7 Conclusion and Discussion

This paper identifies the problem of stealthy bridges between isolated enterprise networks in the public cloud. To infer the existence of stealthy bridges, we propose a two-step approach. A cloud-level attack graph is first built to capture the potential attacks enabled by stealthy bridges. Based on the attack graph, a cross-layer Bayesian network is constructed by identifying uncertainty types existing in attacks exploiting stealthy bridges. The experiments show that the cross-layer Bayesian network is able to infer the existence of stealthy bridges given supporting evidence from other intrusion steps. However, one challenge posed by cloud environments needs further effort. Since the structure of cloud is very dynamic, generating the cloud-level attack graph from scratch whenever a change happens is expensive and time-consuming. Therefore, an incremental algorithm needs to be developed to address such frequent changes such as virtual machine turning on and off, configuration changes, etc.

Disclaimer

This paper is not subject to copyright in the United States. Commercial products are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the identified products are necessarily the best available for the purpose.

Acknowledgements

This work was supported by ARO W911NF-09-1-0525 (MURI), NSF CNS-1223710, NSF CNS-1422594, ARO W911NF-13-1-0421 (MURI), and AFOSR W911NF1210055.

References

[1] Amazon Elastic Compute Cloud (EC2). http://aws.amazon.com/ec2/

[2] Rackspace. http://www.rackspace.com/

[3] Windows Azure: Microsoft's Cloud. https://www.windowsazure.com/en-us/

[4] V. Varadarajan, T. Kooburat, B. Farley, T. Ristenpart, and M. M. Swift, Resource-freeing attacks: improve your cloud performance (at your neighbors expense), ACM CCS 2012.

[5] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, ACM CCS 2009.

[6] D. X. Song, D. Wagner, and X. Tian, Timing Analysis of Keystrokes and Timing Attacks on SSH., in USENIX Security, 2001.

[7] J. Szefer, E. Keller, R. B. Lee, and J. Rexford, Eliminating the Hypervisor Attack Surface for a More Secure Cloud, ACM CCS 2011.

[8] A. Bates, B. Mood, J. Pletcher, H. Pruse, M. Valafar, and K. Butler, Detecting co-residency with active traffic analysis techniques, in CCSW 2012.

[9] J. Dai, X. Sun, and P. Liu. "Patrol: Revealing Zero-Day Attack Paths through Network-Wide System Object Dependencies," ESORICS 2013.

[10] Y. Zhang, A. Juels, A. Oprea, and M. K. Reiter. HomeAlone: Co-residency Detection in the Cloud via Side-Channel Analysis, IEEE S&P 2011.

[11] Y. Chen, V. Paxson, and R. H. Katz, Whats new about cloud computing security. University of California, Berkeley Report No. UCB/EECS-2010-5 January, 2010.

[12] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, Automated generation and analysis of attack graphs, IEEE S&P 2002.

[13] C. R. Ramakrishnan, R. Sekar, and others, Model-based analysis of configuration vulnerabilities, Journal of Computer Security, vol. 10, no. 1/2, pp. 189209, 2002.

[14] C. Phillips and L. P. Swiler, A graph-based system for network-vulnerability analysis, in Proceedings of the 1998 workshop on New security paradigms, 1998.

[15] S. Jajodia, S. Noel, and B. OBerry, Topological analysis of network attack vulnerability, Managing Cyber Threats, pp. 247266, 2005.

[16] P. Ammann, D. Wijesekera, and S. Kaushik, Scalable, graph-based network vulnerability analysis, ACM CCS 2002.

[17] K. Ingols, R. Lippmann, and K. Piwowarski, Practical attack graph generation for network defense, ACSAC 2006.

[18] X. Ou, W. F. Boyer, and M. A. McQueen, A scalable approach to attack graph generation, ACM CCS 2006.

[19] X. Ou, S. Govindavajhala, and A. W. Appel, MulVAL: A logic-based network security analyzer, USENIX Security, 2005.

[20] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, and S. Loureiro, A security analysis of Amazon's elastic compute cloud service, ACM SAC, 2012.

[21] K. Lazri, S. Laniepce, and J. Ben-Othman, Reconsidering Intrusion Monitoring Requirements in Shared Cloud Platforms, ARES 2013.

[22] http://www.snort.org/.

[23] Peng Xie, Jason Li, Xinming Ou, Peng Liu, and Renato Levy. "Using Bayesian networks for cyber security analysis," DSN 2010.

[24] http://www.tenable.com/products/nessus.

[25] http://nvd.nist.gov/.

[26] http://nvd.nist.gov/cvss.cfm.

[27] http://cve.mitre.org/.

[28] http://www.tripwire.com/.

[29] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2446.

[30] https://www.samba.org.

[31] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5423.

[32] https://info.tiki.org/.

[33] http://reasoning.cs.ucla.edu/samiam/.

[34] S. Bugiel, S. Nrnberger, T. Pppelmann, A.-R. Sadeghi, and T. Schneider, AmazonIA: when elasticity snaps back, ACM CCS 2011.

[35] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur. "Bayesian event classification for intrusion detection." ACSAC 2003.

Who Touched My Mission: Towards Probabilistic Mission Impact Assessment

Xiaoyan Sun
Pennsylvania State University
University Park, PA 16802, USA
xzs5052@ist.psu.edu

Anoop Singhal
National Institute of Standards and Technology
Gaithersburg, MD 20899, USA
anoop.singhal@nist.gov

Peng Liu
Pennsylvania State University
University Park, PA 16802, USA
pliu@ist.psu.edu

ABSTRACT

Cyber attacks inevitably generate impacts towards relevant missions. However, concrete methods to accurately evaluate such impacts are rare. In this paper, we propose a probabilistic approach based on Bayesian networks for quantitative mission impact assessment. A System Object Dependency Graph (SODG) is first built to capture the intrusion propagation process at the low operating system level. On top of the SODG, a mission-task-asset (MTA) map can be established to associate the system objects with corresponding tasks and missions. Based on the MTA map, a Bayesian network can be constructed to leverage the collected intrusion evidence and infer the probabilities of tasks and missions being tainted. An example MTA-based BN is provided to show how our approach can enable effective quantitative mission impact assessment.

Categories and Subject Descriptors

K.6.m [**MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS**]: Miscellaneous

General Terms

Security

Keywords

Mission impact assessment; Bayesian network; System Object Dependency Graph

1. INTRODUCTION

Defending missions in cyber space from various attacks continues to be a challenge. An effective attack can lead to great loss in the confidentiality, integrity, or availability to the missions, and even cause some to abort in extreme cases [1]. When an attack happens, one major concern to the security administrators is how the attack could possibly impact related missions. Specifically, they may ask the questions such as 1) How likely is a mission affected? 2) To what extent is the mission influenced? Which tasks are already tainted, and which are untouched?

Continuous efforts have been made to construct high-level models that aid the mission impact analysis, but concrete methods that achieve accurate quantitative assessment are rare. Dai et al. [2] propose a Situation Knowledge Reference Model (SKRM) that enables mission damage and impact assessment. However, without rigidly specifying the cross-layer interconnections, SKRM lacks the capability of performing quantitative mission impact analysis. Jackobson [1] constructs an impact dependency graph (IDG) for mission situation assessment. Nevertheless, the paper doesn't specify detailed method for generating the dependencies in the IDG. The impact assessment provided by the IDG is not sufficiently precise.

In this paper, we propose a probabilistic approach based on Bayesian networks (BN) for mission impact assessment. Our approach is to 1) build a System Object Dependency Graph (SODG) so that the intrusion propagation process is captured at the system object level; 2) construct a Mission-Task-Asset (MTA) map to associate the missions and composing tasks with corresponding assets, which are namely the system objects such as processes, files, etc. The MTA map is naturally connected to the SODG through shared system objects; 3) establish a Bayesian network based on the MTA map and the SODG to leverage the collected intrusion evidence and infer the probabilities of interested events, such as a system object or a mission task being tainted.

The approach is proposed on the basis of the following supporting rationales. First, the SODG is a proper construct connecting the attack and the missions, as shown in Figure 1. From the attack side, an attack's impact towards the operating systems can be reflected on the SODG. System objects that are manipulated directly or indirectly by attackers have the possibility of being tainted. From the mission side, a mission is fulfilled through a sequence of operations towards system objects. These operations are caught by the SODG. As a result, the impact of an attack to the missions can be evaluated by leveraging the SODG as the intermediate bridge.

Second, the SODG is able to capture the intrusion propagation process, which is critical for correct mission impact assessment. An attack's impact towards a mission may not be explicit when they have no common associated assets. The attack-associated assets refer to the system ob-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

SafeConfig'15, October 12, 2015, Denver, Colorado, USA.
© 2015 ACM. ISBN 978-1-4503-3821-9/15/10 ...$15.00.
DOI: http://dx.doi.org/10.1145/2809826.2809834.

Sun, Xiaoyan; Singhal, Anoop; Liu, Peng.
"Who Touched my Mission: Towards Probabilistic Mission Impact Assessment."
Paper presented at the Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig '15), Denver, CO, Oct 12-Oct 12, 2015.

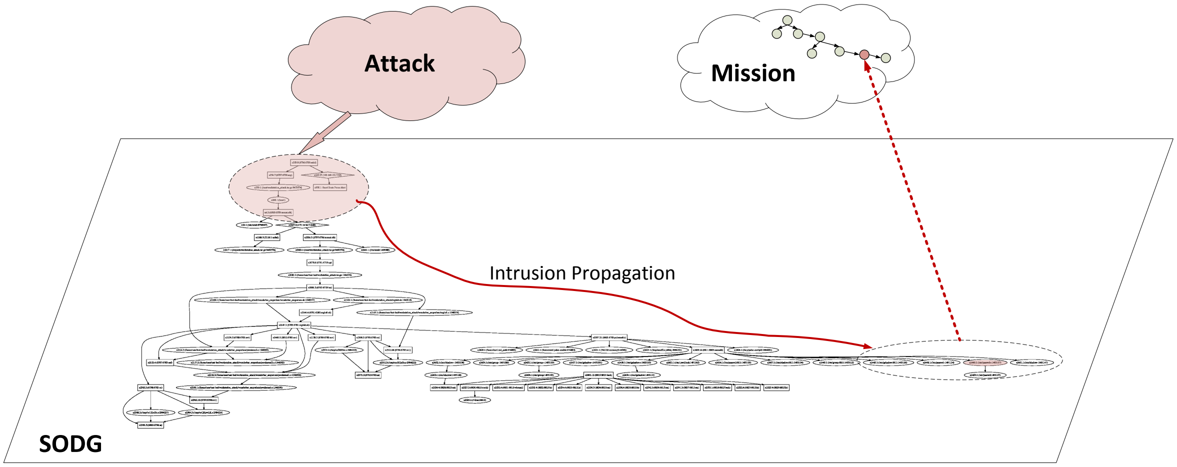


Figure 1: The SODG as the Construct between Attack and Mission [1]

jects that are directly related to the attack activities (e.g. a modified file in a Tripwire [3] alert), while the mission-associated assets refer to the system objects that are involved in the mission commitment. The mission-associated assets do not always share the same system objects with the attack-associated assets, but can still be affected by the latter through intrusion propagation. In this case, the SODG can be employed for tracking the intrusion propagation and assessing the missions that are indirectly affected by the attack-associated assets.

Third, a Bayesian network is able to leverage intrusion evidence to perform probabilistic inference towards interesting events. The evidence can be collected from a variety of information sources, including system logs, security sensors such as Snort [4] and Tcpdump [5], and even human experts.

The paper is organized as follows. Section 2 introduces the System Object Dependency Graph (SODG). Section 3 presents the main principles for establishing the mission-task-asset map. Section 4 briefly discusses the MTA-based Bayesian networks. Section 5 describes the related work. Section 6 concludes the whole paper.

2. THE SYSTEM OBJECT DEPENDENCY GRAPH

In essence, a mission can be decomposed to a set of tasks, which are then committed through a number of operating system operations via system calls, such as read, write, execve, fork, kill, etc. These system calls operate towards system objects like processes, files, and sockets. For instance, the system call *read* can read from a file and *fork* creates a copy of a process. An intrusion usually begins with one or more tainted system objects that are directly or indirectly manipulated by attackers. For example, an execution file containing a Trojan horse may have been installed on a host; a service may have been compromised with a rootkit program and started sending sensitive data back to the attackers' machine; some critical data that influences the control flow could have been corrupted so that the execution paths of a mission workflow can be changed. In subsequent system calls, these intrusion-originating system objects will interact with other innocent objects and get them tainted. This is an *intrusion propagation* process. In this way, the intrusion can propagate across a number of systems inside a network. Among all the system objects tainted via intrusion propagation, some could be the mission-associated ones so that the related tasks will get impacted as well.

Table 1: System Call Dependency Rules

System calls	Dependency
write, pwrite64, rename, mkdir, fchmod, chmod, fchownat, etc.	process→file
stat64, read, pread64, execve, etc.	file→process
vfork, fork, kill, etc.	process→process
write, pwrite64, send, sendmsg, etc.	process→socket
read, pread64,recv, recvmsg, etc.	socket→process
sendmsg, recvmsg, etc.	socket→socket

Given the system call log, a *System Object Dependency Graph (SODG)* can be constructed to capture the intrusion propagation process [8]. Each system call is first parsed into three elements: a source object, a sink object, and a dependency relation between them. This paper applies similar rules, shown in Table 1, as in [6–8] for system call parsing. When constructing the SODG, the parsed objects become nodes and the dependency relations become edges. For example, a *read* system call can be parsed into a process object p, a file object f, and a dependency relation $f \rightarrow p$, meaning that p depends on f.

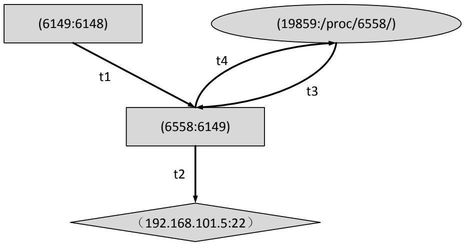
Fig. 2b shows an example SODG built from a simplified system call log in Fig. 2a. Processes, files, and sockets are represented with rectangles, ellipses, and diamonds respectively. A process is often uniquely identified by the process PID *pid* and the parent process PID *ppid*, and thus can be denoted with a tuple (*pid*:*ppid*). Similarly, a file and a socket can be denoted with tuple (*inode*:*path*) and (*addr*:*port*).

The SODG construction process for Figure 2b is as follows. First, the system call *clone* is parsed into a dependency (6149 : 6148)→(6558 : 6149). The dependency be-

[1] The SODG is used to show how the intrusion can propagate from the attack associated assets to the mission assocaited assets. Readers are not expected to understand the details inside the nodes of the SODG.

```
syscall:clone time:t1 pid:6149 ppid:6148 pcmd:bash
cpid:6558  cppid:6149 cpcmd:bash
syscall:write time:t2 pid:6558 ppid:6149 pcmd:sshd
ftype:SOCK addr:192.168.101.5 port:22
syscall:read  time:t3 pid:6558 ppid:6149 pcmd:mount
ftype:REG  path:/proc/6558/ inode:19859
syscall:write time:t4 pid:6558 ppid:6149 pcmd:sshd
ftype:REG  path:/proc/6558/ inode:19859
```

(a) simplified system call log



(b) SODG

Figure 2: An example SODG built from the simplified system call log

comes an edge between the two processes. Second, the system call *write* forms a dependency between a process and a socket: (6558 : 6149)→(192.168.101.5 : 22). The dependency becomes an edge between the process and the socket. Third, the system call *read* indicates that the process then reads a file, and thus creates a dependency (19859 : $/proc/$6558/)→(6558 : 6149). Finally, the process writes back to the same file, and forms a dependency (19859 : $/proc/$6558/)←(6558 : 6149).

After the SODG is constructed, forward and backward tracking can be performed to identify the potentially tainted objects. Since an attack can often cause security sensors to raise alerts, the system objects involved in these alerts can be used as the trigger points that start the tracking process. For example, if Tripwire raises an alert that a file is modified abnormally, then the file can be used as a trigger point. On the SODG, the file is marked as tainted. Starting from this file, forward and backward tracking can be performed to generate an intrusion propagation path [8]. The objects on this path are very likely to be tainted.

3. MISSION-TASK-ASSET MAP

Constructing Mission-Task-Asset (MTA) map is to relate the system objects with the tasks and missions. An intuitive solution is to decompose the missions into tasks, and further associate the tasks with system objects. However, this top-down decomposing approach requires the prior knowledge of a mission workflow. In cases when attackers are able to insert malicious tasks into the workflow, these inserted tasks could be missed by the MTA map.

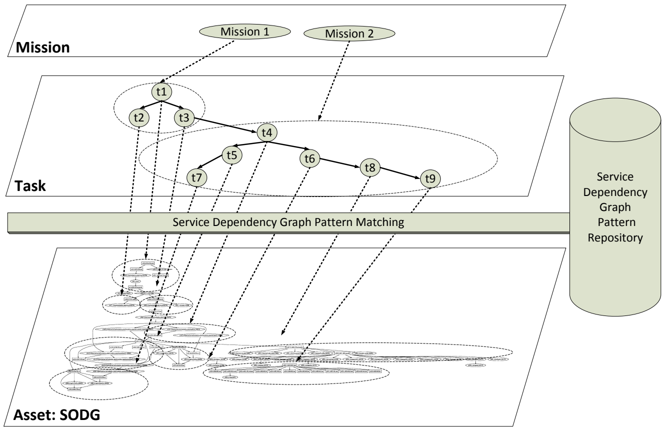

Mission
Mission 1
Mission 2
t1
t2
t3
t4
t5
t6
t7
t8
t9
Task
Service Dependency Graph Pattern Matching
Service Dependency Graph Pattern Repository
Asset: SODG

Figure 3: Mission-Task-Asset Map [2]

In this paper, we propose a *bottom-up extraction* approach that extracts the tasks from the SODG, and then relates the tasks with specific missions, as shown in Figure 3. Since the SODG captures what actually happens in the network, extraction from the SODG accurately reflects which tasks are actually committed. Considering the manageable number of missions and tasks an enterprise network could deal with, relating tasks with missions is not a real issue. The key difficulty lies in how to extract tasks from the SODG due to its daunting size. However, the extraction is ensured to be feasible by the following principles.

First, a mission task can be viewed as an instantiation of several services that have dependency relations. In enterprise networks, the normal function of a service may depend on one or more other services. These services and applications often interact and work together to accomplish specific tasks. For example, a user's login request requires web service from a web server, which further relies on au authentication service to verify the user's legitimacy. The authentication will then depend on the database service to access the users' account information. In this example, a single task "user login" can be viewed as the instantiation of combined web service, authentication service, and database service. Therefore, if such dependency relations among services can be discovered and represented with specific graphs, then a task can be viewed as the instantiation of a service dependency graph.

Second, through service discovery, the service dependency graphs (SDGs) can be established at the system object level. Service discovery has been studied intensively in previous work [9–12]. Dai [13] proposed to infer the service dependency through identifying OS-level causal paths. Therefore, the service dependencies can be represented with OS-level dependency graphs, such as the SODGs. Each service dependency graph has a pattern that can be used to identify the corresponding SDG. The patterns could be defined from the perspective of both text and graph-topology. For example, a file node with name *config* and an out degree of n can be one feature for a specific pattern, indicating that file *config* is accessed n times. Since servers in an enterprise network often fulfill routine responsibilities, the common patterns can be extracted to form an SDG pattern repository.

[2] Again, readers are not expected to understand the details inside the nodes of the SODG.

Third, the system assets can be linked to tasks automatically by matching the SODG against the SDG patterns. Although the SODG is usually not human-readable, it can be annotated with specific SDGs through pattern matching. For example, if the pattern for combined web service, authentication service, and database service appears in the SODG for several times, then as the instantiations of these services, several "user login" tasks can be linked to the system objects involved in these patterns.

4. BAYESIAN NETWORKS

To perform probabilistic mission impact assessment, the Bayesian networks can be constructed based on the established MTA maps. The Bayesian network is a type of Directed Acyclic Graph that can be used to model the cause and effect relations. In a BN, the nodes represent the variables of interest, and the edges represent the causality relations between nodes. The strength of such causality relations can be specified with conditional probability tables (CPT). When evidence is provided, a properly constructed BN can infer the probabilities of interesting variables.

In this paper, we propose to construct an MTA-based BN, whose input is the intrusion evidence collected from various security sensors, and output is the probabilities of interesting security events, such as a system object or a task being tainted. The graphical feature of MTA enables and facilitates the construction of MTA-based BN. With CPT tables specified and the evidence incorporated, the MTA-based BN is able to infer the probabilities of tasks and missions being tainted, and thus evaluate the impact of attacks towards interesting missions.

To build the MTA-based BN, the dependency relations existing in the MTA map need to be well modeled. Each MTA map implies certain dependency relations among the missions, tasks, and system objects. Such dependency relations can be represented with certain mission dependency graphs by interpreting the MTA maps. In the mission dependency graph, the status of a mission depends on the status of the composing tasks, while the status of a task depends on the status of the relevant system objects. We provide two example mission dependency graphs based on the same MTA map to illustrate how the dependency relations can be interpreted.

Figure 4 is an example of benign mission dependency graph by interpreting an MTA map. In this graph, a mission is composed of several tasks. For each mission to be benign, all of its composing tasks should be benign. In addition, all the tasks should be committed in the correct sequence. Similarly, each task is also composed of several system level operations. To ensure the task is benign, the related system objects should be benign and the operations should be performed in the right sequence. Therefore, all of the parent nodes have the "AND" relation for the child node to be true. In Figure 4, Node 5 "Task 1 is benign" should have 4 preconditions satisfied in order to be true: Node 1, F1 is benign; Node 2, P1 is benign; Node 3, F2 is benign; Node 4, "Process P1 reads File F1" happens before "Process P1 writes File F2", meaning that the read operation is executed before the write operation. In this example, in order for Node 5 to become true, all the relevant system objects are benign and all the system operations are performed in the right sequence. The relationship between these conditions (Node 1 to 4) is "AND".

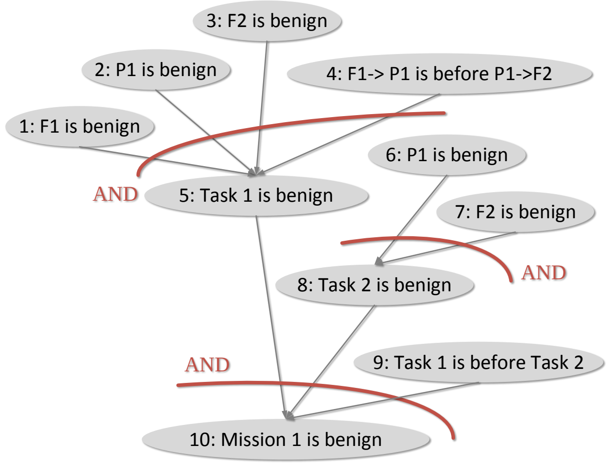


Figure 4: An Example of Benign Mission Dependency Graph

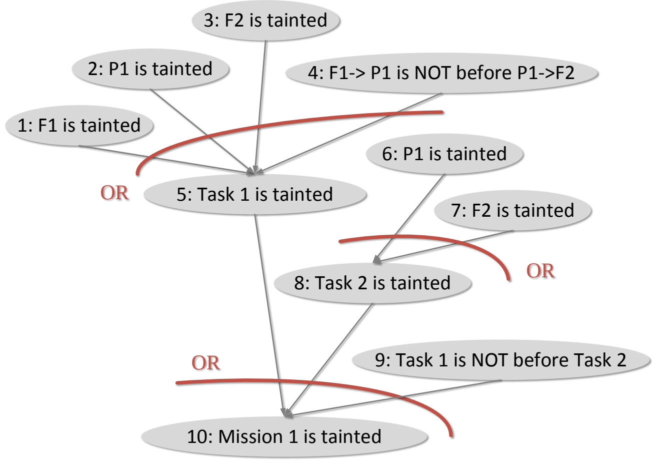


Figure 5: An Example of Tainted Mission Dependency Graph

Figure 5 is an example of a tainted mission dependency graph by interpreting the same MTA map as in Figure 4. In this graph, if any of the system objects are tainted or the system operations are not performed in the right order, the associated task can be marked as tainted. Similarly, if any of the tasks are tainted or not committed in the correct sequence, the associated mission is tainted. Therefore, all the parent nodes have the "OR" relation for the child node to be true, meaning any of the preconditions being true could cause the post-condition effective. For example, even if only F1 in Node 1 is tainted while F2 and P1 are still benign, Task 1 will get tainted, which will further impacts Mission 1.

To model the above "AND" and "OR" relations, a MTA-based BN can be constructed as shown in Figure 6. Instead of specifying the taint status of objects, tasks, and missions

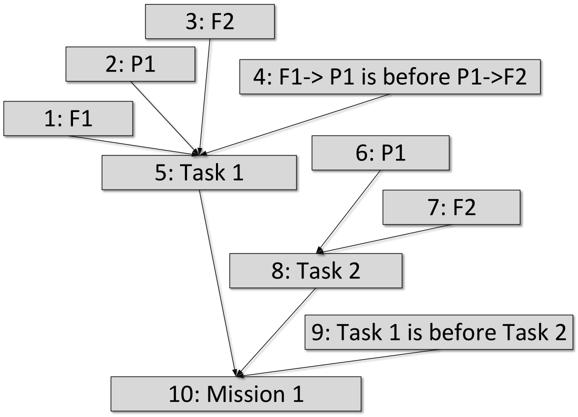


Figure 6: An Example of MTA-based BN

in the nodes directly, the MTA-based BN specify the states in the CPT tables. For example, the CPT table for Mission 1 in Figure 6 is shown in Table 2. In this table, Mission 1, Task 1, and Task 2 have possible states of "tainted" and "not tainted". The operation sequence "Task 1 is before Task 2" in Node 9 has the states of "true" and "false". Other potential states, such as "clear but in danger", or "not sure", etc, could also be assigned for system objects depending on specific situations.

In addition, the numbers in Table 2 modeled the "AND" and "OR" relations. For example, to get "mission 1 = not tainted" the probability of 1, all the three conditions "Task 1 is tainted", "Task 2 is tainted", and "Task 1 is before Task 2" have to be false. As long as any of these three conditions are true, the probability for "mission 1 = tainted" will become 1. If the three conditions have different impact on the mission's taint status, the numbers in the CPT table can be modified accordingly to reflect such difference. For example, in Table 3, "Task 1 is tainted" has greater impact on missions than the other two conditions. When "Task 1 is tainted", the probability for the mission being tainted is bigger than 0.9, no matter if the other conditions are true or false. When Task 1 is not tainted, the probability for the mission being tainted is very low, even if task 2 is tainted or the operation sequence is incorrect. The CPT table can also be modified to accommodate other noise factors that cannot be completely taken into consideration. For example, in Table 3, even if all the three conditions are true, the probability of mission 1 being tainted may not be 1, but a number very close to 1, such as 0.99.

After the BN is constructed, the taint status of system objects is input into BN as evidence. The BN then computes the probabilities of missions being infected based on the given evidence.

5. RELATED WORK

Mission Impact Assessment. Some high level frameworks and models have been established in recent studies to enable qualitative evaluation towards cyber attacks' impact on missions. Alberts et al. [15] proposed a Mission Assurance Analysis Protocol (MAAP) to determine how the current conditions can affect a project. Watters et al. [16] proposed a Risk-to-Mission Assessment Process to map the network nodes to the business objectives. Musman et al. [14] clarified the cyber mission impact assessment framework and related the business processes with technology capacities. Dai et al. [2] proposed a Situation Knowledge Reference Model (SKRM) that enables capabilities such as asset classification, mission damage and impact assessment. [1] is one of the few works that explore quantitative mission impact assessment. It presented an impact-oriented cyber attack model, where an attack has an impact factor and the asset is measured with operational capacity. The assets' operational capacity will be affected by the attack's impact factor. The paper then briefly introduced the impact dependency graph (IDG), but didn't provide details for the construction method.

Bayesian Network. Bayesian networks have been employed in a number of studies for cyber security defense. [17] presented a BN modeling approach which modeled three uncertainty types in the security analysis process. The BN was constructed on top of the logical attack graphs [18, 19]. [20] proposed to construct a cross-layer Bayesian network to infer stealthy bridges existing between the enterprise network islands in cloud. [21] described a mission-impact-based approach to correlate the security alarms collected from different sensors using Bayesian networks. An incident rank tree was built to calculate the rank of each security alert, which combines the incident's impact towards the mission, and the success probability of the activity reported in the alert. Our work also applies Bayesian networks, but targets a different problem.

6. CONCLUSION

This paper proposed a probabilistic approach to evaluate the impacts towards missions caused by attacks. To associate attacks with system assets, a System Object Dependency Graph (SODG) can be built to reflect the influence of attacks towards system objects and capture the intrusion propagation to other objects as well. To further relate the assets with missions, we proposed to buid a mission-task-asset (MTA) map based on the SODG so that the attacks' impact towards system objects can propagate to the related missions. We provided an example Bayesian network that is constructed on top of the MTA to show how our approach can be applied to infer the probabilities of missions being tainted.

Acknowledgement

This work was supported by NIST 70NANB14H218, ARO W911NF-09-1-0525 (MURI), NSF CNS-1422594, and ARO W911NF-13-1-0421 (MURI).

Disclaimer

This paper is not subject to copyright in the United States. Commercial products are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National

Table 2: CPT of Mission 1 in the Figure 6

Mission1	Task 1=Tainted				Task 1=Untainted			
	Task 2=Tainted		Task 2=Untainted		Task 2=Tainted		Task 2=Untainted	
	C = True	C = False	C = True	C = False	C = True	C = False	C = True	C = False
Tainted	1	1	1	1	1	1	1	0
Untainted	0	0	0	0	0	0	0	1

Note: C represents the condition "Task 1 is committed before Task 2"

Table 3: Modified CPT of Mission 1 in the Figure 6

Mission1	Task 1=Tainted				Task 1=Untainted			
	Task 2=Tainted		Task 2=Untainted		Task 2=Tainted		Task 2=Untainted	
	C = True	C = False	C = True	C = False	C = True	C = False	C = True	C = False
Tainted	0.99	0.9	0.9	0.9	0.2	0.2	0.2	0.01
Untainted	0.01	0.1	0.1	0.10	0.8	0.8	0.8	0.99

Note: C represents the condition "Task 1 is committed before Task 2"

Institute of Standards and Technology, nor does it imply that the identified products are necessarily the best available for the purpose.

7. REFERENCES

[1] Gabriel Jakobson. Mission Cyber Security Situation Assessment Using Impact Dependency Graphs.

[2] Jun Dai, Xiaoyan Sun, Peng Liu, Nicklaus Giacobe. Gaining Big Picture Awareness through an Interconnected Cross-layer Situation Knowledge Reference Model. 2012 ASE International Conference on Cyber Security, Washington DC, 2012

[3] Tripwire. http://www.tripwire.com/.

[4] Snort. https://www.snort.org/.

[5] Tcpdump. http://www.tcpdump.org/.

[6] S. T. King, and P. M. Chen. Backtracking intrusions. ACM SIGOPS, 2003.

[7] X. Xiong, X. Jia, and P. Liu. Shelf: Preserving business continuity and availability in an intrusion recovery system. ACSAC, 2009.

[8] J. Dai, X. Sun, and P. Liu. Patrol: Revealing zero-day attack paths through network-wide system object dependencies. ESORICS, 2013.

[9] A. Natarajan, P. Ning, Y. Liu, S. Jajodia, and S.E. Hutchinson. NSDMiner: Automated discovery of Network Service Dependencies. In Proceeding of IEEE International Conference on Computer Communications, 2012.

[10] Barry Peddycord III, Peng Ning, and Sushil Jajodia. On the accurate identifi- cation of network service dependencies in distributed systems. In USENIX Association Proceedings of the 26th international conference on Large Installation System Administration: strategies, tools, and techniques, 2012.

[11] Rodrigo Fonseca, George Porter, Randy H. Katz, Scott Shenker, and Ion Stoica. X-trace: A pervasive network tracing framework. In USENIX Association Proceedings of the 4th USENIX conference on Networked systems design and implementation, 2007.

[12] Paul Barham, Richard Black, Moises Goldszmidt, Rebecca Isaacs, John Mac- Cormick, Richard Mortier, and Aleksandr Simma. Constellation: automated discovery of service and host dependencies in networked systems. In TechReport MSR-TR-2008-67, 2008.

[13] Jun Dai. Gaining Big Picture Awareness in Enterprise Cyber Security Defense. Ph.D. dissertation, 2014.

[14] S. Musman, A. Temin, M. Tanner, D. Fox, and B. Pridemore. Evaluating the Impact of Cyber Attacks on Missions. MITRE Technical Paper 09-4577, July 2010.

[15] Alberts C., et al. (2005). Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments. CMU/SEI-2005-TN-032. Pittsburgh, PA: Carnegie Mellon University.

[16] Watters J., et al. (2009). The Risk-to-Mission Assessment Process (RiskMAP): A Sensitivity Analysis and an Extension to Treat Confidentiality Issues.

[17] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy. Using Bayesian networks for cyber security analysis. DSN, 2010.

[18] X. Ou, W. F. Boyer, and M. A. McQueen. A scalable approach to attack graph generation. ACM CCS, 2006.

[19] X. Ou, S. Govindavajhala, and A. W. Appel. MulVAL: A Logic-based Network Security Analyzer. USENIX security, 2005.

[20] Xiaoyan Sun, Jun Dai, Anoop Singhal, Peng Liu. Inferring the Stealthy Bridges between Enterprise Network Islands in Cloud Using Cross-Layer Bayesian Networks 10th International Conference on Security and Privacy in Communication Networks (SecureComm 2014), Beijing, China

[21] M. Fong, P. Porras, and A. Valdes. A Mission-Impact-Based Approach to INFOSEC Alarm Correlation. Proceedings Recent Advances in Intrusion Detection. Zurich, Switzerland, October 2002.

Sun, Xiaoyan; Singhal, Anoop; Liu, Peng.
"Who Touched my Mission: Towards Probabilistic Mission Impact Assessment."
Paper presented at the Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig '15), Denver, CO, Oct 12-Oct 12, 2015.

Kinetics of Photodegradation and Nanoparticle Surface Accumulation of a Nanosilica/Epoxy Coating Exposed to UV Light

Lipiin Sung,[1] Justin M. Gorham,[2] Deborah Stanley,[1] Hsiang-Chun Hsueh,[1] Savelas Rabb,[2] Lee L. Yu,[2] Chun-Chieh Tien[1] and Tinh Nguyen[1]

[1]Engineering Laboratory
[2]Material Measurement Laboratory
National Institute of Standards and Technology, Gaithersburg, MD, USA

Abstract

Temperature effect on the kinetics of photodegradation, surface accumulation of nanoparticles, and nanoparticle release in an epoxy nanocoating exposed to ultraviolet light (UV) was investigated. A model epoxy coating containing 5 % untreated nanosilica was selected. Exposed film specimens were removed at specified UV dose intervals for measurements of chemical degradation of the epoxy component, nanosilica accumulation on specimen surface, and nanosilica release as a function of UV dose for four temperatures. The chemical degradation was measured using Fourier transform infrared spectroscopy (FTIR), X-ray photoelectron spectroscopy (XPS), and UV-visible spectroscopy (UV-Vis). Atomic force microscopy (AFM) was employed to determine the kinetics of nanosilica accumulation on the nanocoating surface during UV exposure. The temperature dependence behaviors of kinetic parameters obtained by various measurement techniques will be used to better understand the degradation mechanism and surface accumulation of nanoparticles in exterior nanocoatings.

SP-951
Sung, Li Piin; Gorham, Justin; Jacobs, Deborah; Rabb, Savelas; Yu, Lee; Nguyen, Tinh.
"Kinetics of Photodegradation and Nanoparticle Surface Accumulation of a Nanosilica/Epoxy Coating Exposed to UV Light."
Paper presented at the American Coatings Conference, Indianapolis, IN, Apr 11-Apr 13, 2016.

INTRODUCTION

Polymeric materials containing nanofillers (polymer nanocomposites) have attracted growing interest due to their outstanding properties as well as their unique applications[1-5]. Polymer nanocoatings, a subclass of nanocomposites, are increasingly used outdoors such as on building structures, airplanes, and automobiles, because of their excellent mechanical, gas barrier, self–cleaning, and UV resistance properties.

Studies have long indicated that most common polymers undergo significant degradation during exposures to outdoor environments [6-8]. A serious consequence of the matrix degradation for nanocoatings is that the nanofillers embedded in the polymer matrices could be released via the effect of rain, snow, condensed water, and wind. Such nanoparticle release during nanocoating life cycle is a concern, because engineered nanofillers have been shown to be hazardous to the environment and human health [9-11].

Taking advantage of the highly uniform and high intensity UV radiation from the SPHERE device (Simulated Photodegradation *via* High Energy Radiant Exposure) [12], the National Institute of Standards and Technology (NIST) has investigated the degradation rate, nanomaterial surface accumulation, and nanomaterial release for a model epoxy (without UV stabilizers) containing silica nanoparticles [13-16]. In a previous study on an amine-cured epoxy nanocoating exposed to UV radiation at 60 ^{o}C/≈ 0 % relative humidity (RH) exposure condition, we have found that the epoxy matrix in the nanocoating underwent rapid photodegradation during exposure to 295 nm to 400 nm UV, exposing nanosilica on the surface and subsequently releasing it from the nanocoating [13].

Although nanosilica accumulated on the surface and subsequent release from the nanocoatings was observed and measured [13], the role of temperature on the photodegradation rate, surface accumulation and release of nanoparticles has not been investigated. Temperature is an important factor in the degradation process of polymers. In this study, we examined how temperature affects the both the photodegradation of polymer matrix and surface accumulation (and possible release) of nanosilica during UV exposures of an epoxy nanocoating. The resulting knowledge of temperature dependence behaviors on kinetic parameters obtained by different measurements will be useful for understanding the degradation mechanism and predicting the long term release of nanoparticles in exterior nanocoatings.

EXPERIMENTAL PROCEDURES

Materials and Preparation of Nanocoating

Unless stated, the silica nanoparticles (i.e., nanosilica) were an untreated material in powder form, having a normal diameter of 15 nm and a purity greater than 99.5 % (provided by manufacturer). The epoxy coating was a model stoichiometric mixture of a diglycidyl ether of bisphenol A (DGEBA) epoxy resin having an equivalent mass of 189 (grams of resin containing one gram equivalent of epoxide) and a tri-polyetheramine curing agent. There were no UV stabilizers added to the amine-cured epoxy coating. It should be noted that, due to steric hindrance and restricted transport during the late curing stages, some residual unreacted epoxide and amino groups are expected to be present in the coating films after curing. The presence of these functional groups and impurities (e.g., residual catalysts, processing aids, etc.) may have an influence on the photodegradation of an amine-cured epoxy coating. The solvent used for nanoparticle dispersion and coating processing was reagent grade toluene (purity > 99.5 %). The chemical structures of the components and the cured epoxy coating are given elsewhere [16]. Free-standing films having a thickness between 125 μm and 150 μm of the amine-cured epoxy containing 5 % mass fraction of nanosilica were prepared following the procedure described in Ref. [15]. All films were cured at ambient conditions (24 °C and 50 % RH) for 1 d, followed by post-curing for 45 min at 110 °C in an air circulating oven. The quality of all epoxy/nanosilica coating (epoxy nanocoating) films was assessed by visual inspection for evidence of air bubbles or defects (cracks). Specimens were only selected from defect-free regions.

UV Exposure

Specimens of epoxy nanocoating were exposed to < 1 % RH at four different temperatures, 30 °C, 40 °C, 50 °C, and 60 °C in the NIST SPHERE UV chamber [12]. The very dry condition was used to minimize any effect of water on the photodegradation of epoxy. The NIST SPHERE UV chamber produces a highly uniform UV flux of approximately 140 W/m^2 in the wavelength range of 295 nm to 400 nm. Specimens for characterizing surface morphology had a dimension of 10 mm x 10 mm and those for tracking chemical changes had a diameter of 19 mm Specimens were removed after specified accumulated UV doses (i.e., at specified time intervals) for various characterizations. UV dose, in MJ/m^2, is defined here as the total accumulated energy resulting from repeated UV radiation exposures at a particular time period per unit irradiated surface. Because the SPHERE was operated without interruption during this experiment, its UV dose is linearly proportional to exposure time.

Characterization of Nanocoating Degradation and Surface Morphological changes

The chemical degradation of both neat epoxy and nanocoating was measured using molecular spectroscopy via attenuated total reflection Fourier transform infrared spectroscopy (ATR-FTIR), X-ray photoelectron spectroscopy (XPS), and UV-visible spectroscopy (UV-Vis). ATR-FTIR spectra were recorded at a resolution of 4 cm^{-1} using dry air as a purge gas and a spectrometer (Nexus 670, Thermo Nicolet) equipped with a liquid nitrogen-cooled mercury cadmium telluride (MCT) detector. A ZnSe prism and 45° incident angle were used for the ATR-FTIR measurement. All spectra were the average of 128 scans. The peak height was used to represent the infrared intensity, which is expressed in absorbance, A. All FTIR results were the average of four specimens. UV-Visible spectra were recorded using an HP 8452A spectrometer fitted with an autosampler. Spectra were collected for wavelengths from 190 nm to 1100 nm with an integration time of 0.5 s.

XPS was used for elemental and chemical state analysis of the nanocoatings. Analyses were carried out using an Axis Ultra DLD spectrophotomer (Kratos Analytical) equipped with a monochromated Al Kα X-ray source (1486.6 eV). The photoelectrons were collected along the surface normal at a pass energy 40 eV and a step size of 0.1 eV/step for the C(1s), Si(2p), O(1s) and N(1s) regions. All XPS spectra were fit with a Shirley baseline and adjusted with the appropriate elemental sensitivity factors to obtain information on percent composition.

Surface morphological changes of nanocoating were followed by tapping mode atomic force microscopy (AFM) at ambient conditions (24 °C, 50 % RH) using a Dimension 3100 system (Veeco Metrology) and silicon probes (TESP 70, Veeco Metrology). Both topographic (height) and phase images were obtained simultaneously using a resonance frequency of approximately 300 kHz for the probe oscillation and a free-oscillation amplitude of 62 nm ± 2 nm.

RESULTS

Surface Morphological Changes

Figure 1 displays AFM height and phase images of unexposed and UV-exposed epoxy nanocoating surface at, as an example, 40 °C. Contrast in the height images of Figure 1a is due to the surface topography, with little evidence of nanoscale particles being present on the surface, which is also confirmed in the featureless phase image (Figure 1a, right). As the UV dose increased, the surface roughness increased and nanoparticles or clusters of nanoparticles appeared on the surface, as shown in both the height and phase images of Figure 1b. Brightness of the particles in the height image indicates that they were above the surface. The phase image also shows a strong contrast between the nanoparticles and the matrix, which is typically observed for mixtures of a high modulus inorganic material and a low modulus polymeric material.

Figure 2 shows the surface morphological changes of the nanocoating exposed to different UV doses in four temperatures (30 °C, 40 °C, 50 °C, and 60 °C). All four temperatures showed similar effects. The number of particles on the surface increased with increasing UV dose, and the size of the particle clusters and the number of connected clusters also increased with UV dose. After 400 MJ/m^2 dose, a layer of compact particles almost covered the entire surface for all four temperatures. Similar results were observed in NIST previous studies for a silane-treated nanosilica in a similar epoxy system [8, 16].

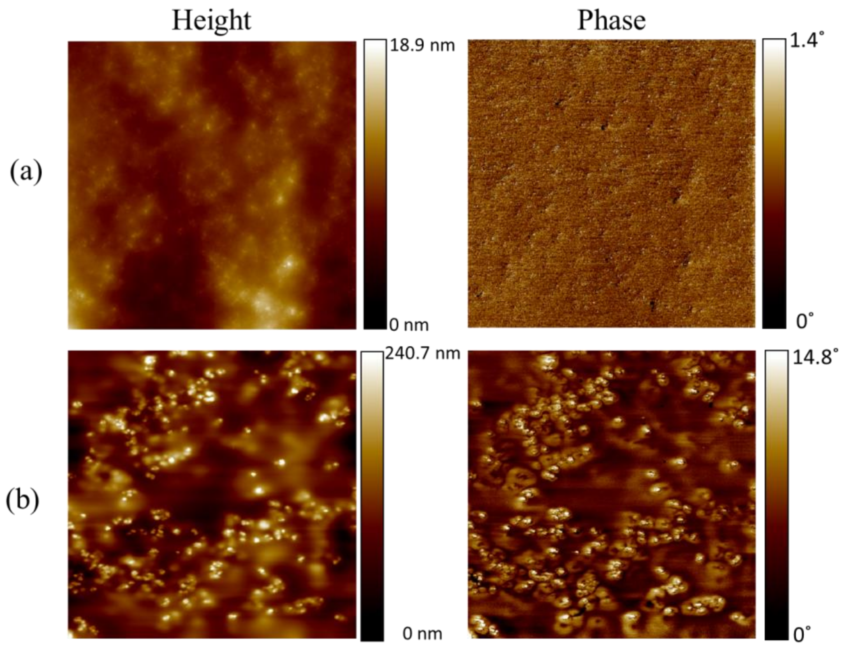


Figure 1 AFM height images (left column) and phase images (right column) of nanocoating (a) unexposed and (b) exposed for 30 MJ/m^2 UV dose and at 40 °C. Scan size is 20 μm × 20 μm. The scale bars represent the height and phase range of each image.

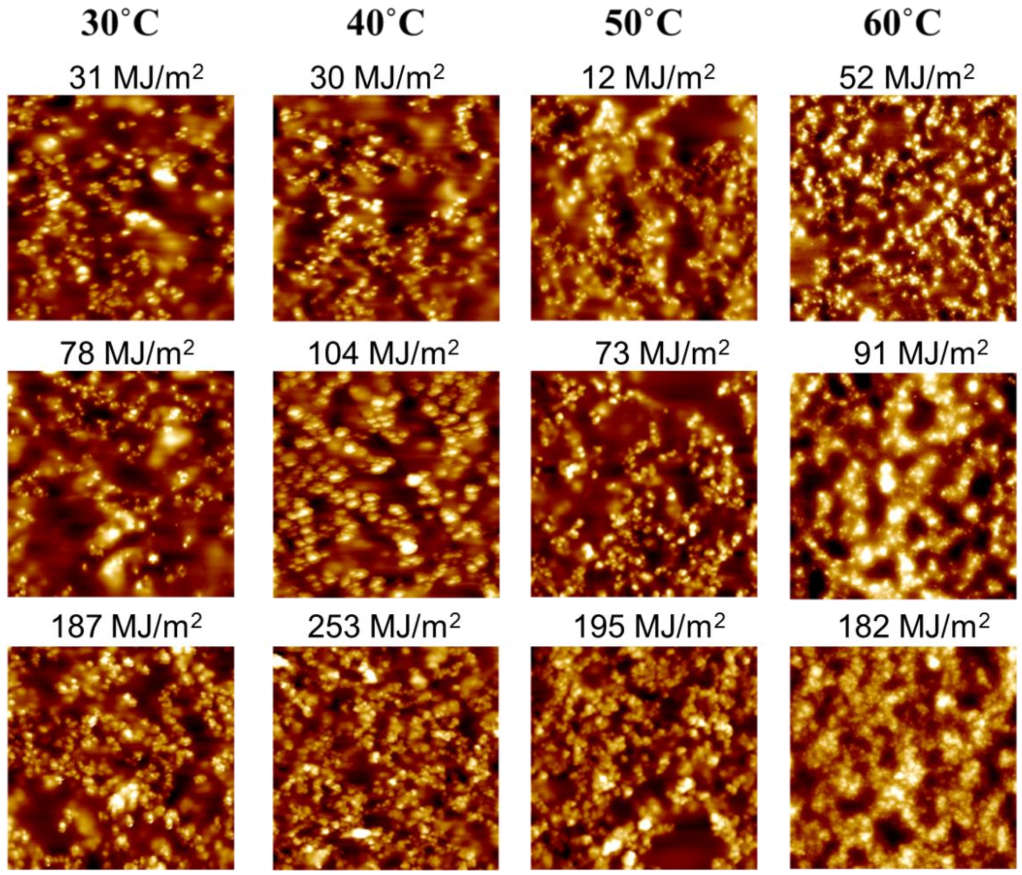


Figure 2: AFM height images of epoxy nanocoating as a function of UV doses for four different temperatures; scan size: 20 μm × 20 μm. The height range of the images are roughly from 0 nm to 1.5 μm.

To follow the accumulation of nanosilica on the nanocoating surface during UV exposure, an AFM software image analysis was conducted. Figure 3 displays the surface coverage (in %) of revealed particles (assuming as nanosilica clusters) as a function of UV dose. It shows that the accumulation of nanosilica on the UV-exposed nanocoating increased rapidly between 0 MJ/m^2 and 300 MJ/m^2 dose but slowed down substantially thereafter. The shape of nanosilica coverage vs. UV dose curve is similar to the chemical changes such as oxidation measured by FTIR with UV dose [13], suggesting that the accumulation of nanosilica on the nanocoating surface with UV exposure is closely related to photodegradation of the epoxy matrix. That is, as the epoxy layer on the nanocoating surface was degraded by UV radiation, silica nanoparticles that were embedded in the matrix were increasingly exposed on the surface. Figure 3 shows that a higher exposure temperature resulted in a higher amount of surface accumulation of nanosilica for dose less than 600 MJ/m^2. For example, at an exposure dose of 400 MJ/m^2, the surface coverages were approximately 45 %, 50 %, 56 %, and 60 % for 30 °C,40 °C, 50 °C, and 60 °C, respectively. However, at doses of 700 MJ/m^2 or greater, there was essentially no difference in surface coverage between 50 °C and 60 °C.

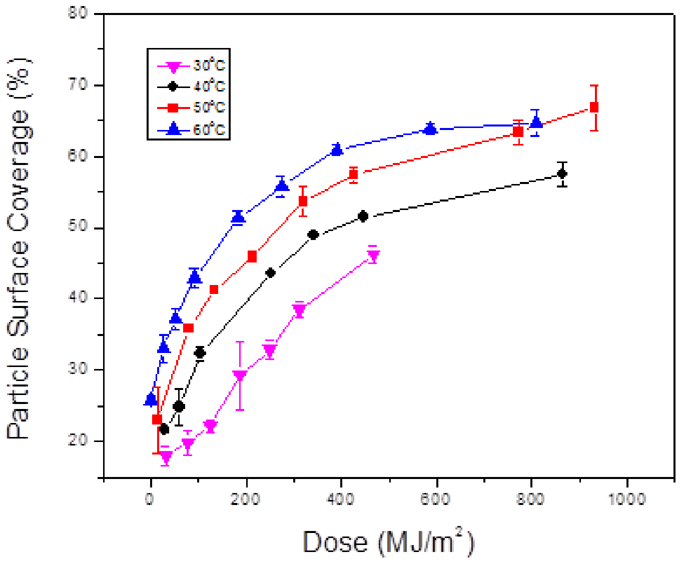


Figure 3. Nanosilica coverage on epoxy nanocoating surface as a function of UV dose at four different temperatures as indicated in the legend. Each data point is the average of three measurements (20 µm × 20 µm scan area). The error bars represent one standard deviation.

Chemical Degradation

Figure 4 displays the chemical degradation of an amine-cured epoxy nanocoating exposed to UV radiation at four different temperatures measured by FTIR-ATR technique. The bands at 1245 cm^{-1} and 1724 cm^{-1}, representing chain scission and oxidation of the epoxy, respectively, and at 1060 cm^{-1}, attributed to both epoxy C-O and Si-O bonds, were used to follow various degradation processes and surface accumulation of silica nanoparticles of nanocoating during UV exposure. Intensity changes of these bands after normalization to 1380 cm^{-1} with UV dose are displayed in Figure 4. The error bars in Figure 4 show small standard deviations (except at high UV dose), indicating a good reproducibility between specimens. Detailed description of FTIR data analyses was reported in Reference [13]. As shown in Figures 4a and 4b, the intensity of the bands at 1245 cm^{-1} and 1724 cm^{-1} changed rapidly at shorter/lower exposure time/dose (< 200 MJ/m^2), but reached a plateau value for dose > 400 MJ/m^2. The 60 °C data shows a highest degradation rate (a fewer data points than other temperature because of rapid degradation) among the four temperatures. The intensity of the band at 1060 cm^{-1} (Figure 4c) increased with increasing UV dose, suggesting that silica has gradually accumulated on the specimen surface. However, there was no clear trend in the temperature effect on this combined C-O and Si-O band. This is probably a result of two oppositely competing processes taking place on the nanocomposite surface during UV irradiation: loss of epoxy material (C-O loss) and increase of silica nanoparticles on the surface (Si-O increase).

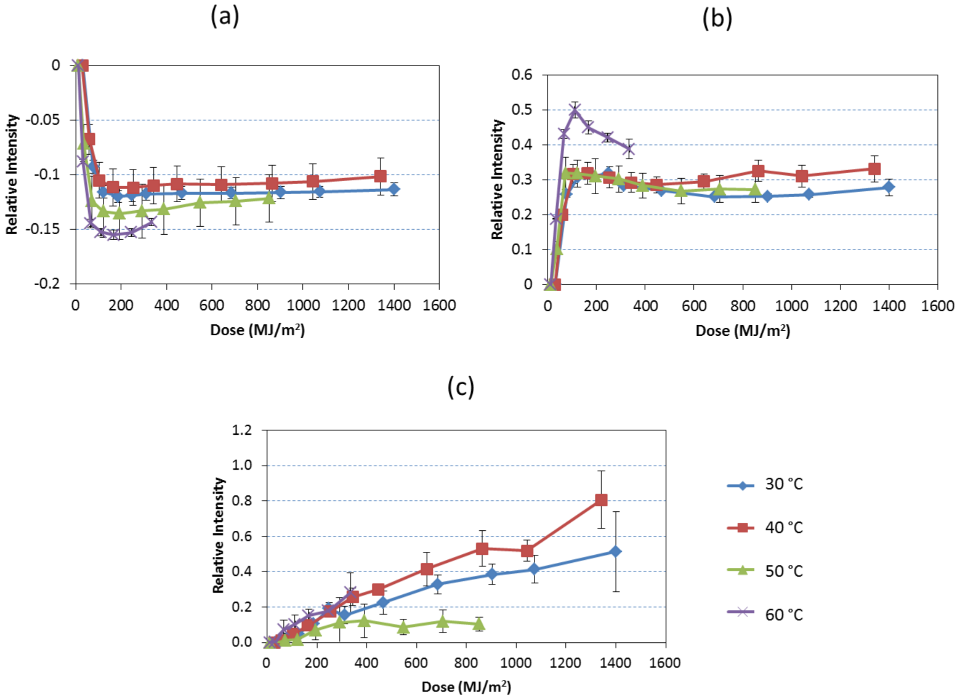


Figure 4. ATR-FTIR relative intensity changes with UV dose at four temperatures for bands at: a) 1245 cm^{-1}, b) 1724 cm^{-1}, and c) 1060 cm^{-1}. The intensities have been normalized to that of the band at 1380 cm^{-1}. The results are average of 6 specimens, and error bars represent one standard deviation.

In addition to FTIR data, UV-Vis measurements were also carried out on thinner nanocoating specimens (a 7 µm film on a CaF_2 substrate) to obtain the chemical degradation rate at various exposure temperatures. Figure 5 displays the chemical changes via UV-Vis absorbance at wavelength (λ) = 354 nm for both neat epoxy and nanocoatings at four different exposure temperatures. In both materials, the absorbance increased as UV dose increased, and higher temperature had a higher rate of increase.

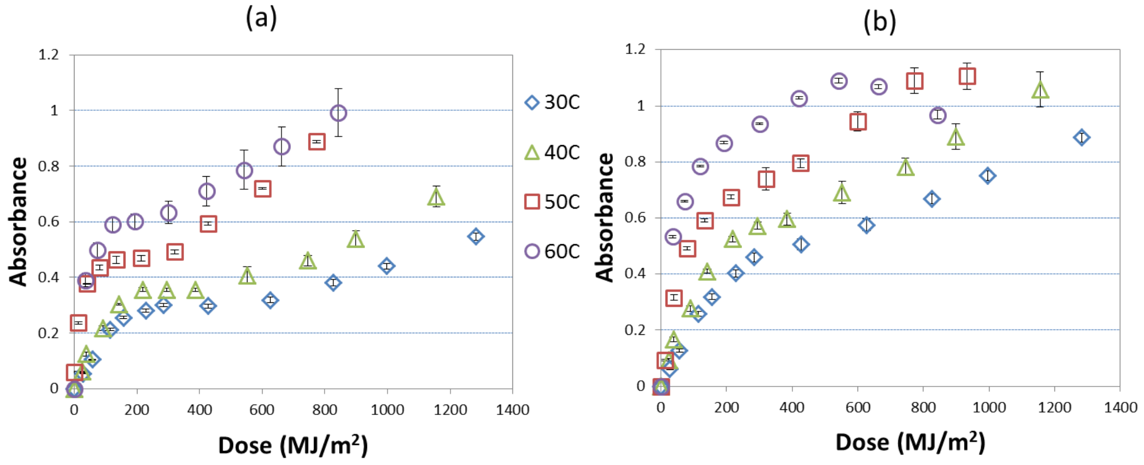


Figure 5. UV-visible intensity at λ = 354 nm as a function of UV dose for (a) neat epoxy and (b) nanocoating for four different temperatures. The results are average of 4 specimens, and error bars represent one standard deviation. All absorbance values presented here are subtraction from values at exposure time =0.

To detect the chemical composition on the nanocoating surface, XPS measurements were performed on the same samples after AFM measurements. Figure 6 displays the XPS-based carbon (C), oxygen (O), nitrogen (N), and silicon atomic (Si) percentages on the epoxy/nanosilica coating surface vs. exposure time. The loss of the epoxy matrix and an increase of the silica material near the nanocoating surface as a function of exposure time (proportional to dose) observed by ATR-FTIR in Figure 4a and 4c are consistent with the XPS results displayed in Figure 6. As the UV dose increased from 0 MJ/m^2 to 770 MJ/m^2 (≈ 60 d) at 60 °C exposure condition, the percent surface concentrations of carbon decreased from 77.4 % ± 1.4 % to 50.2 % ± 1.7 %, while those of silicon started at 3.4 % ± 0.8 %, dropped after a small dose of 54 MJ/m^2 to 0.9 % ± 0.1 % followed by a steady rise to a final value of 6.5 % ± 0.4 %, and nitrogen increased from 1.4 % ± 0.2 % to 8.1 % ± 0.2 %. The increase of nitrogen with UV dose observed in Figure 6 for nanosilica composite may be explained as due to the adsorption of the base amine curing agent on the acidic nanosilica surface during mixing and film formation. In this case, the adsorbed amine would form an interfacial layer between the silica nanoparticles and the epoxy polymer. Discussion on the formation of this interfacial layer is described in Ref [13].

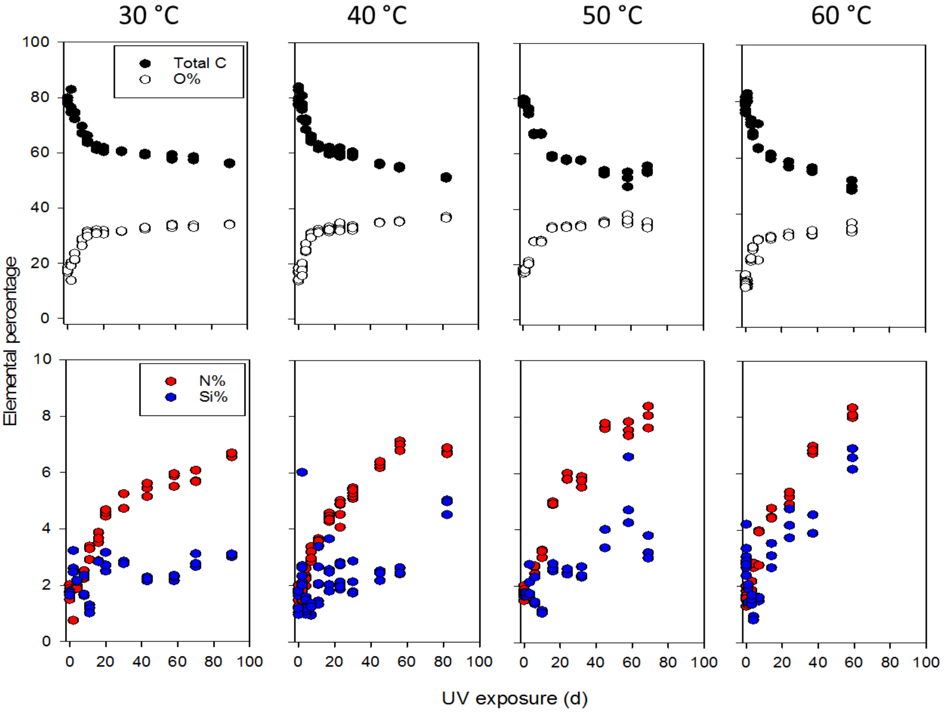


Figure 6. XPS-based carbon, nitrogen, and silicon atomic percentages on the epoxy/nanosilica coatings surface vs. UV exposure time (d). At same exposure times, more than two locations were measured as shown in the graphs.

To get a better comparison visually, the increase of Si element percentage at different temperatures was plotted vs. UV dose for four different temperatures; the results are displayed in Figure 7. For doses less than 200 MJ/m^2, all data scatterred around 2 % with large error bars for all temperatures. Expect for 50 °C exposure condition, the data do not follow a steady increase with temperature, and the last data point drop unexpectedly. In general, a higher exposure temperature resulted in a higher amount of Si element percentage for doses > 200 MJ/m^2. However, the Si(2p) percentages increased with UV dose at a rate that increased with temperature. Extrapolated based on a linear fit of measurements (dose > 0 MJ/m^2) at each temperature (not shown), the Si percentage that is at the surface for 600 MJ/m^2 is 2.5 % ± 0.1 %,, 2.8 % ± 0.2 %, 3.6% ± 0.3 %, and 5.4 % ± 0.4 % for 30 °C, 40 °C, 50 °C, and 60 °C, respectively. This result is in agreement with nanosilica surface accumulation data obtained by AFM measurements shown in Figure 3.

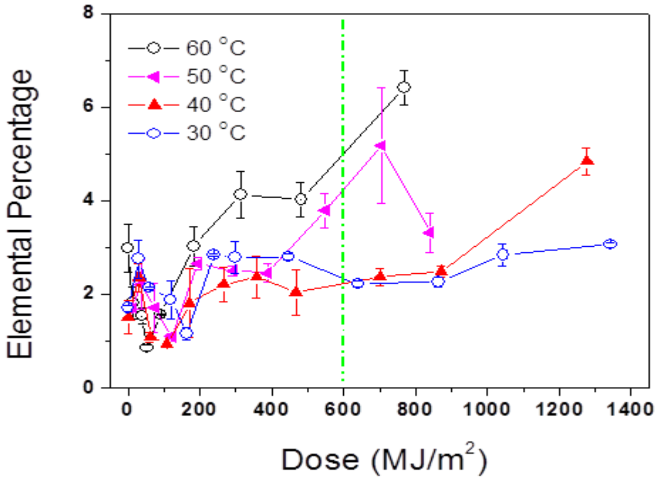


Figure 7. XPS-based silicon (Si) % elemental percentage on the epoxy/nanosilica coatings surface vs. UV irradiation dose at four different temperatures. Each data point consists of two or more specimens and the error bars represent one standard deviation. The dashed line indicates the dose at 600 MJ/m^2.

CONCLUDING REMARKS

The effects of temperature on both the photodegradation of epoxy matrix and surface accumulation of nanosilica during UV exposures of an epoxy coating containing 5 mass % nanosilica were investigated through a suite of techniques, such as FTIR, XPS, UV-Vis, and AFM. All results indicated that the higher temperature, the higher photodegradation and surface nanosilica accumulation rate. The chemical degradation rate of the matrix (via FTIR data in Figures 4a & 4b, UV-Vis data in Figure 5), and accumlation rate for Si on the surface (via AFM: Figure 3 and via XPS data in Figure 6) followed the right temperature order, i.e., 60 °C > 50 °C > 40 °C > 30 °C. Further data analyses are on going to obtain degradation kinetic parameters for nanocoatings exposed to various UV/temperature/humidity conditions. Kinetics data of polymer coatings containing nanoparticles under different UV environments is essential for better understanding the degradation mechanism and predicting the release of nanopartices from exterior nanocoatings.

DISCLAIMER

Certain commercial product or equipment is described in this paper in order to specify adequately the experimental procedure. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that it is necessarily the best available for the purpose.

REFERENCE

[1] Podsiadlo, P, Kaushik, AK, Arruda, EM, Waas, AM, Shim, BS, Xu, J, et al., "Ultrastrong and stiff layered polymer nanocomposites," *Science,* vol. 318, pp. 80-3, Oct 5 2007.

[2] Crosby, AJ, and Lee, YJ "Polymer Nanocomposites: The “Nano” Effect on Mechanical Properties," *Polymer Reviews,* vol. 47, pp. 217-229, 2007.

[3] Croce, F, Appetecchi, G, Persi, L, and Scrosati, B, "Nanocomposite polymer electrolytes for lithium batteries," *Nature,* vol. 394, pp. 456-458, 1998.

[4] Ramanathan, T, Abdala, AA, Stankovich, S, Dikin, DA, Herrera-Alonso, M, Piner, RD*, et al.*, "Functionalized graphene sheets for polymer nanocomposites," *Nat Nanotechnol,* vol. 3, pp. 327-31, Jun 2008.

[5] Shah, MSA, Nag, M, Kalagara, T, Singh,S, and Manorama, S V, "Silver on PEG-PU-TiO2 polymer nanocomposite films: An excellent system for antibacterial applications," *Chemistry of Materials,* vol. 20, pp. 2455-2460, 2008.

[6] Sung, LP, Jasmin, J, Gu, XH, Nguyen,T, and Martin, JW, "Use of laser scanning confocal microscopy for characterizing changes in film thickness and local surface morphology of UV-exposed polymer coatings," *J. Coat. Technol. Res.,* vol. 1, pp. 267-276, 2004.

[7] Nguyen, T, Martin, J, Byrd, E, and Embree, N,"Relating laboratory and outdoor exposure of coatingsIII. Effect of relative humidity on moisture-enhanced photolysis of acrylic-melamine coatings," *Polymer Degradation and Stability,* vol. 77, pp. 1-16, 2002.

[8] Nguyen,T, Pellegrin,B, Bernard, C, Gu, X, Gorham, JM, Stutzman, P*, et al.*, "Fate of nanoparticles during life cycle of polymer nanocomposites," *Journal of Physics: Conference Series,* vol. 304, p. 012060, 2011.

[9] Jin, Y, Kannan, S, Wu, M, and Zhao, JX, "Toxicity of luminescent silica nanoparticles to living cells," *Chem Res Toxicol,* vol. 20, pp. 1126-33, Aug 2007.

[10] Lin, W, Huang, JW, Zhou, XD, and Ma, Y, "In vitro toxicity of silica nanoparticles in human lung cancer cells," *Toxicol Appl Pharmacol,* vol. 217, pp. 252-9, Dec 15 2006.

[11] Lin, YS, and Haynes, CL, "Impacts of mesoporous silica nanoparticle size, pore ordering, and pore integrity on hemolytic activity," *J Am Chem Soc,* vol. 132, pp. 4834-42, Apr 7, 2010.

[12] Chin, J, Byrd, E, Embree,E, et al., “Accelerated UV weathering device based on integrating sphere technology,”. Rev. Sci. Instrum. Vol. 75, pp. 4951-4959, 2004.

[13] Sung, L, Stanley, D, Gorham, JM, Rabb, SA, Gu, X, Yu, LL, Nguyen, T, “A quantitative study of nanoparticle release from nanocoatings exposed to UV radiation,” *J. Coat. Technol. Res., Vol.* 12, no1, pp. 121-135, 2015.

[14] Nguyen, T, Pellegrin, B, Bernard, C, Gu, X, Gorham, JM, Stutzman, P, Stanley, D, Shapiro, A, Byrd, E, Hettenhouser, R, Chin, J, “Fate of nanoparticles during life cycle of polymer nanocomposites,” J. Phys.: Conf. Ser., 304 012060, 2011.

[15] Gorham, JM, Nguyen, T, Bernard, C, Stanley, D, Holbrook, RD, “Photo-induced surface transformations of silica nanocomposites,” Surf. Interface Anal., Vol. 44, pp. 1572-158, 2012.

[16] Nguyen, T, Pellegrin, B, Bernard, C, Rabb, S, Stutzman, P, Gorham, JM, Gu, X, Yu, LL, Chin, J, “Characterization of surface accumulation and release of nanosilica during irradiation of polymer nanocomposites by ultraviolet light.” J. Nanosci. Nanotechnol., Vol. 12, pp. 6202-6215, 2012.

[17] Stanley, D, Huang, SR, Cheng, YL, Rabb, S, Gorham, JM, Krommenhoek, PJ, Yu, LL, Nguyen, T and Sung, L, “Investigating the Process of Surface Degradation and Nanoparticle Release of a Commercial Nanosilica / Polyurethane Coating Under UV Exposure,” Accepted for *publication, J. Coat. Technol. Res.,* Dec., 2015.

Procedia Computer Science
Volume 80, 2016, Pages 386–397
ICCS 2016. The International Conference on Computational Science

A Hybrid Human-Computer Approach to the Extraction of Scientific Facts from the Literature

Roselyne B. Tchoua[1], Kyle Chard[2], Debra Audus[3], Jian Qin[4], Juan de Pablo[5], and Ian Foster[1,2,6]

[1] Department of Computer Science, The University of Chicago, Chicago, IL, USA
roselyne@uchicago.edu
[2] The Computation Institute, The University of Chicago and Argonne, Chicago, IL, USA
[3] The National Institute of Standards and Technology, Gaithersburg, MD, USA
[4] Department of Chemical Engineering, Stanford University, Stanford, CA 94305
[5] Institute for Molecular Engineering, The University of Chicago, Chicago, IL, USA
[6] Math and Computer Science Division, Argonne National Laboratory, Argonne, IL, USA

Abstract

A wealth of valuable data is locked within the millions of research articles published each year. Reading and extracting pertinent information from those articles has become an unmanageable task for scientists. This problem hinders scientific progress by making it hard to build on results buried in literature. Moreover, these data are loosely structured, encoded in manuscripts of various formats, embedded in different content types, and are, in general, not machine accessible. We present a hybrid human-computer solution for semi-automatically extracting scientific facts from literature. This solution combines an automated discovery, download, and extraction phase with a semi-expert crowd assembled from students to extract specific scientific facts. To evaluate our approach we apply it to a challenging molecular engineering scenario, extraction of a polymer property: the Flory-Huggins interaction parameter. We demonstrate useful contributions to a comprehensive database of polymer properties.

Keywords: Crowdsourcing, Information Extraction, Classification, Flory-Huggins, Materials Science

1 Introduction

The amount of scientific literature published every year is growing at a prolific rate. Some studies count more than 28,000 scientific journals and 1.8 million articles published annually [19]. As a result, the amount of information (e.g., experimental results) embedded within the literature is overwhelming. It has become impractical for humans to read and extract pertinent information. This problem hinders the advancement of science, making it hard to build on existing results buried in the literature. It also makes it difficult to translate results into applications

Selection and peer-review under responsibility of the Scientific Programme Committee of ICCS 2016
© The Authors. Published by Elsevier B.V.

doi:10.1016/j.procs.2016.05.338

Tchoua, Roselyne; Chard, Kyle; Audus, Debra; Qin, Jian; de Pablo, Juan; Foster, Ian.
“A Hybrid Human-Computer Approach to the Extraction of Scientific Facts From the Literature.”
Paper presented at ICCS 2016: The International Conference on Computational Science, San Diego, CA, Jun 6-Jun 8, 2016.

and thus to produce valuable products. In materials science and chemistry, for example, difficulties discovering published materials properties directly affect the design of new materials [6]. Indeed, despite the many publications in this domain, the process of designing new materials is still one of trial and error. Access to a structured, queryable database of materials properties would facilitate the design and model validation of new substances, improving efficiency by enabling scientists and engineers to more quickly discover, query, and compare properties of existing compounds. At the very least, it would transform an avalanche of publications into a machine-accessible and human-consumable source of knowledge.

Historically, materials properties have been collected in human-curated review articles and handbooks (e.g., the *Physical Properties of Polymers Handbook* [7], the *Polymer Handbook* [18]). However, this approach is laborious and expensive, and thus such collections are published infrequently. We contend that a better approach is to leverage information extraction techniques to process thousands of papers and output structured content for human consumption. To this end, we have developed a semi-automated system, χDB, which, with moderate input from humans, can extract materials properties for the scientific community.

We initially target extraction of a fundamental thermodynamic property called the Flory-Huggins interaction (or χ) parameter, which characterizes the miscibility of polymer blends. We chose to work with this property as a test case as it is particularly challenging to extract, due to the fact that it is published in heterogeneous data formats (e.g., text, figures, tables) and is represented in several different temperature-dependent expressions. To address these challenges, we developed a workflow consisting of an automated Web information extraction phase followed by a crowdsourced curation phase. The output of this workflow is a high quality human- and machine-accessible *digital handbook* of polymer properties. We show that we are able, using only a small group of students, to create a high quality database of properties with more χ values than in other notable handbooks. We expect that our approach is likely also to work well for other materials properties and in other scientific domains.

The rest of this paper is organized as follows. Section 2 presents background information related to Flory-Huggins theory and polymer science. Section 3 discusses related approaches that support automated extraction. Section 4 describes the χDB architecture. Section 5 presents the data collected via crowdsourcing. Section 6 explores the application of machine learning algorithms to improve the automatic selection of χ-relevant publications. Finally, we conclude and discuss future work in Section 7.

2 Application Background

The initial focus of our work is the extraction of properties of particular polymers blends (e.g, χ parameter and glassification temperature). Although highly curated properties database exist for hard [8] and metallic [17] materials, no equivalent exists for polymers blends. However, there is a clear need for a trusted, up-to-date, and easily accessible databases of properties within the soft matter community.

Polymers are large molecules (macromolecules) composed of many repeating units. Since polymeric materials are both ubiquitous and typically consist of several polymeric components, which are generally incompatible, the χ parameter represents a key property in the design of next-generation materials. A database of χ values would allow researchers to make informed judgments as to which χ values and thermodynamic analysis to use when predicting and understanding the phase behavior of multi-component polymeric materials. However, while there are thousands of published χ parameters, there is little consensus regarding the values. Different measurement methods yield different values, and different groups have at times reported

Tchoua, Roselyne; Chard, Kyle; Audus, Debra; Qin, Jian; de Pablo, Juan; Foster, Ian.
"A Hybrid Human-Computer Approach to the Extraction of Scientific Facts From the Literature."
Paper presented at ICCS 2016: The International Conference on Computational Science, San Diego, CA, Jun 6-Jun 8, 2016.

different values for the same polymers. The χ parameter depends on the temperature and the types of polymer(s) or solvent(s) involved. Consequently, many experimental methods have been developed to quantify the temperature dependence of χ, and tabulated values are commonly found in standard textbooks and polymer data handbooks [7, 18]. However, many of these values have not been updated to include recent findings. Moreover, the list of polymer blends found in textbooks is not exhaustive; for example the previously mentioned handbook contains χ values for only 41 polymer-polymer blends. These considerations motivate our goal to collect and store χ values from materials literature into a digital, searchable database. Each record would also include the source and the measurement methodology.

3 Related Work

We review here current practice for building collections of scientific facts, populating scientific databases, information extraction, and crowdsourcing.

Major scientific databases have emerged in various fields where data is growing at exponential rates and the need for data sharing is recognized by the community, notably in biotechnology [2, 9]. In materials science, the Materials Project [8] provides access to large numbers of computed values. For polymers, the expert-curated *Physical Properties of Polymers Handbook* [7], last published in 2007, is a valuable source of data. However, while a valuable resource, it lacks recent results from the literature and does not contain an exhaustive list of polymers.

Information extraction (IE) from text has been extensively studied [5]. IE aims to extract structured information from unstructured and semi-structured documents. It often focuses primarily on extracting information from written language via natural language processing [4]. Sub-disciplines include Web IE [1] and IE from PDF documents and images. Web IE leverages the inherent structure in HTML rather than grammatical rules to extract semantically meaningful information. Web IE approaches work well when extracting information from many pages with the same structure (e.g., real estate listings); however, they do not work well for heterogeneous web pages or when page structure changes [10]. Extracting information from other data types, such as images and PDFs, is particularly difficult. In the case of images, variations in texture, contrast, font size, style and color, orientation, alignment, etc., all impact the extraction process. Similarly, PDF files, while easy to understand for humans, are not designed for machine accessibility. Thus, it is challenging to extract information from embedded items—such as tables and equations—due to the lack of structure in the document. For example, extraction of tables from PDF documents typically relies on identifying cell borders and attempting to map text locations relative to these borders. As tables differ significantly between documents, a considerable amount of human assistance is needed to achieve good results.

One solution to the challenges associated with PDF files is to use experts to identify and correct errors [15]. Indeed, given inaccuracies in IE methods, many IE systems rely on teams of people to review and curate extracted information [14]. Such *crowdsourcing* approaches leverage the fact that humans perform certain tasks better than computers, an idea also exploited in systems such as Galaxy Zoo [12], for image labeling in astronomy; the Amazon Mechanical Turk micro-task marketplace [3], and the Wikipedia online encyclopedia.

4 χDB Architecture and Implementation

Mining the literature for a loosely structured property such as the χ parameter requires extracting values from a variety of objects, including text, figures, tables, and equations; processing the many different forms in which the property occurs, e.g., a single number at a given temperature or a linear equation as a function of temperature; and identifying associated information such as the polymers and solvents involved, their molecular masses, the temperature(s) at which experiments were performed, the methods used, and any error estimates. Thus, the techniques used to find, extract and store χ must be flexible.

Given these multiple levels of complexity, we have developed χDB—a hybrid machine-human system that leverages both automatic extraction and expert human review via crowdsourcing. The χDB workflow shown in Figure 1 comprises three main phases: automatic download and first-level extraction of publications; crowdsourced extraction and review (the "review process") of χ values, and finally the exposure of a curated database of χ values (the "Digital Handbook of Properties"). In the rest of this section, we define the χDB data model and then describe the system architecture used to realize each of these workflow phases.

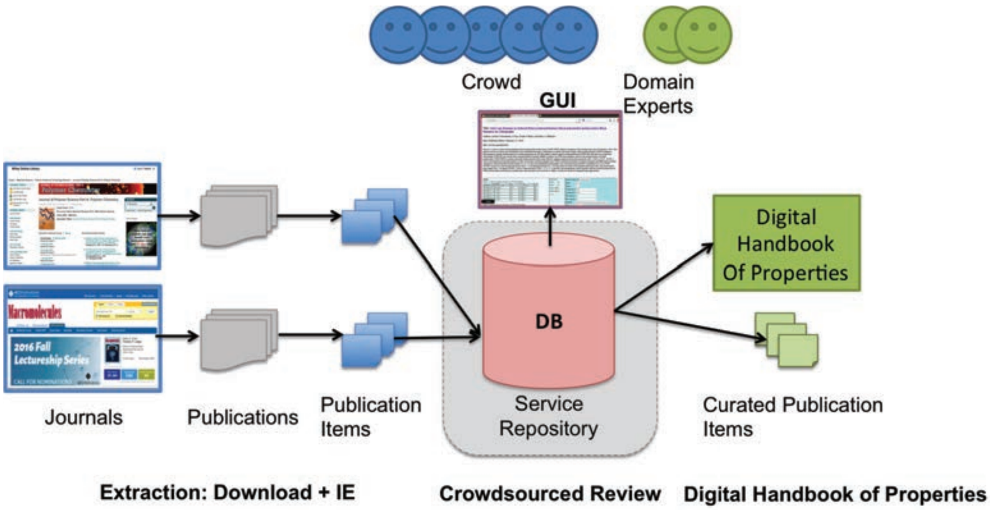

Crowd
Domain Experts
GUI
Digital Handbook Of Properties
DB
Journals
Publications
Publication Items
Service Repository
Curated Publication Items
Extraction: Download + IE
Crowdsourced Review
Digital Handbook of Properties

Figure 1: χDB architecture

4.1 Data Model

The χDB data model is designed to represent (1) the complex extraction and review workflow, (2) the various temperature-dependent formats in which χ occurs, and (3) the complete provenance of each extracted value. To model the different users' reviews the data model includes a representation of publications before, during, and after reviews, as well as a data model for the multiple representations of χ. The χDB data model includes seven core tables: `papers` (extracted publications), `items` (extracted publication items), `sources` and `reviewed_sources` (reviewed information before and after consensus), `chis` and `reviewed_chis` (χ values before and after consensus), and `reviewed_papers` (classified papers). One challenge when defining the data model is the need to support different representations in which χ is specified. After reviewing the literature we developed a data model that could include four main representations of χ: 1) a number at a specific temperature; 2) a linear equation in terms of temperature: $\chi = A + \frac{B}{T}$; 3) a quadratic equation in terms of temperature: $\chi = A + \frac{B}{T} + \frac{C}{T^2}$; 4) a number that combines χ and N, where N is proportional to the degree of polymerization or molecular weight: χN; and a final catch-all class, 5) other representations.

4.2 Extraction

χDB first discovers and downloads relevant publications—in this case publications that contain the keyword *Flory-Huggins*—from suitable journals. It then uses an HTML tag parser to extract structured publication metadata, including Digital Object Identifier (DOI), title, authors, and date of publication. This information is used to index the publication such that it can be linked to other stored information (e.g., referenced values in other papers). Finally, the publication is parsed into *items* (e.g., abstract, figures, tables, equations, text) that are separately downloaded and can be reviewed individually. Links between publication items and their originating publication are maintained so that they can be displayed to reviewers in a coherent manner. The full text and the original URL are also stored such that reviewers and users can retrieve the original publication.

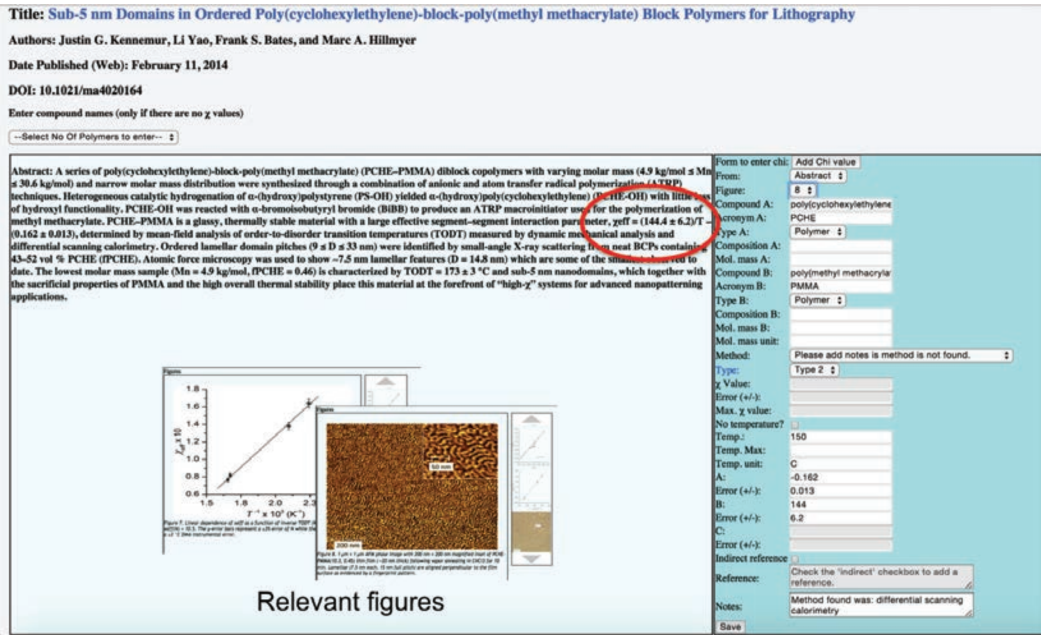
We implemented this phase in three components: a Python web crawler (to discover relevant publications), a downloader (to download a copy of the publication), and a WebIE extractor (to extract metadata and items from the publication). We initially focused on *Macromolecules*, a leading scientific journal on polymers. The crawler is configured to use the *Macromolecules* search capabilities to prioritize downloads. After discussion with experts, we chose the search term *Flory-Huggins* and specified a date range from January 2010. The crawler returns a ranked list of publications. The downloader uses these results to download each publication (as an HTML file) using the URL returned by the crawler. The downloader extracts relevant metadata from the structured web page (DOI, title, authors, etc.) Finally, a Python WebIE script parses the HTML to detect and extract items from the publication (e.g., abstract, images, equations, and tables). The abstract and the HTML tables are stored directly in the χDB database. Figures and equations are downloaded and referenced in the database.

4.3 Crowdsourced Review

To assemble a crowd for reviewing extractions we developed a materials science course that combined teaching the fundamentals of polymer chemistry and physics and reviewing the literature containing χ parameters. The reviewing component of the course tasked the students with extracting χ parameters using the χDB system. This involved reviewing the free-text publication, and entering any χ values that they identified.

We implemented this phase as a PHP-based web service and PHP/HTML website. Due to copyright restrictions, the reviewing components of χDB are accessible only within the University of Chicago network. The review interface includes two main pages: a list of all publications with assigned reviewers and a review page for reviewing publications and items. We implemented a consensus-based review process using two reviewers per paper to reduce error. We rely on a second class of reviewers (experts) to resolve conflicting reviews.

An individual review consists of scanning extracted items for χ values. Once identified, reviewers are asked to extract χ values from all of these items, with the exception of figures as extractions from figures are likely to be inaccurate. The reviewer enters each extracted χ value in an online form. The item from which a value is extracted is marked as *relevant*. Note: items may be marked as *relevant* even if they do not contain any χ values. For example, a *relevant* figure may be a phase diagram or a micrograph of the material; a *relevant* table may contain supporting information. If a paper contains a single χ value or a single *relevant* item, it is also marked as *relevant*. Consequently, a paper that contains neither is classified as *irrelevant*. Figure 2 shows an example of the review form. To ensure that the resulting database is unambiguous, we define a set of minimum required information for submission of a χ value. Some χ values are embedded directly in the text (rather than in an extracted item); therefore



Title: Sub-5 nm Domains in Ordered Poly(cyclohexylethylene)-block-poly(methyl methacrylate) Block Polymers for Lithography

Authors: Justin G. Kennemur, Li Yao, Frank S. Bates, and Marc A. Hillmyer

Date Published (Web): February 11, 2014

DOI: 10.1021/ma4020164

Enter compound names (only if there are no χ values)

--Select No Of Polymers to enter--

Abstract: A series of poly(cyclohexylethylene)-block-poly(methyl methacrylate) (PCHE–PMMA) diblock copolymers with varying molar mass (4.9 kg/mol ≤ Mn ≤ 30.6 kg/mol) and narrow molar mass distribution were synthesized through a combination of anionic and atom transfer radical polymerization (ATRP) techniques. Heterogeneous catalytic hydrogenation of α-(hydroxy)polystyrene (PS-OH) yielded α-(hydroxy)poly(cyclohexylethylene) (PCHE-OH) with little loss of hydroxyl functionality. PCHE-OH was reacted with α-bromoisobutyryl bromide (BiBB) to produce an ATRP macroinitiator used for the polymerization of methyl methacrylate. PCHE–PMMA is a glassy, thermally stable material with a large effective segment–segment interaction parameter, χeff = (144.4 ± 6.2)/T – (0.162 ± 0.013), determined by mean-field analysis of order-to-disorder transition temperatures (TODT) measured by dynamic mechanical analysis and differential scanning calorimetry. Ordered lamellar domain pitches (9 ≤ D ≤ 33 nm) were identified by small-angle X-ray scattering from neat BCPs containing 43–52 vol % PCHE (fPCHE). Atomic force microscopy was used to show ~7.5 nm lamellar features (D = 14.8 nm) which are some of the smallest observed to date. The lowest molar mass sample (Mn = 4.9 kg/mol, fPCHE = 0.46) is characterized by TODT = 173 ± 3 °C and sub-5 nm nanodomains, which together with the sacrificial properties of PMMA and the high overall thermal stability place this material at the forefront of "high-χ" systems for advanced nanopatterning applications.

Form to enter chi:	Add Chi value
From:	Abstract
Figure:	8
Compound A:	poly(cyclohexylethylene
Acronym A:	PCHE
Type A:	Polymer
Composition A:	
Mol. mass A:	
Compound B:	poly(methyl methacrylat
Acronym B:	PMMA
Type B:	Polymer
Composition B:	
Mol. mass B:	
Mol. mass unit:	
Method:	Please add notes is method is not found.
Type:	Type 2
χ Value:	
Error (+/-):	
Max. χ value:	
No temperature?	□
Temp.:	150
Temp. Max:	
Temp. unit:	C
A:	-0.162
Error (+/-):	0.013
B:	144
Error (+/-):	6.2
C:	
Error (+/-):	
Indirect reference	□
Reference:	Check the 'indirect' checkbox to add a reference.
Notes:	Method found was: differential scanning calorimetry

Figure 2: Screenshot of the χDB Graphical User Interface with the χ entry form enabled

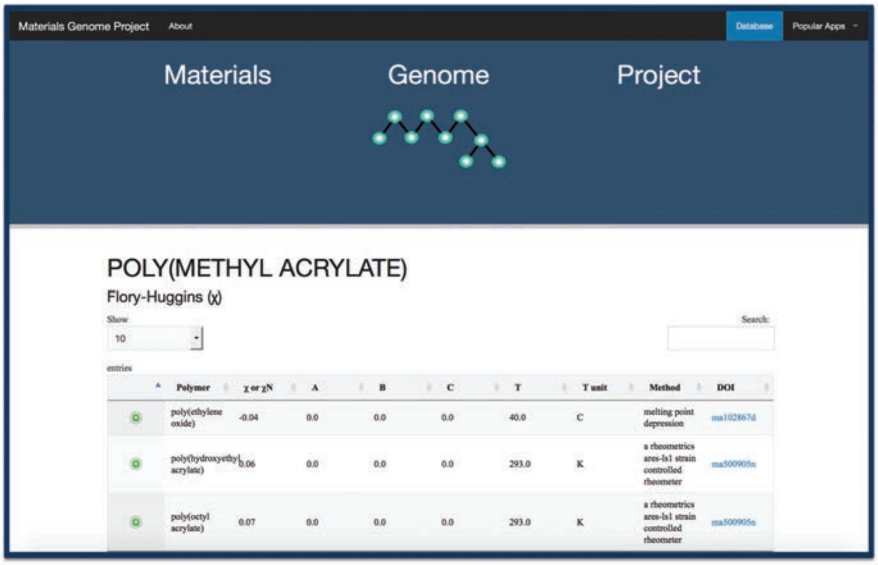
reviewers are able to retrieve the full text article via the link on the review page. If additional χ values are found in the full text, reviewers click the "Add Chi" button next to the abstract with the possibility to indicate in the form that the value was actually extracted from the main text. Second reviews of the same publications consist of a similar process, however second reviewers are able to view the previous reviewers' input before submitting their own, giving them the opportunity to identify errors or conflicts between reviews. In the case of errors, the interface allows submission of either review; in the case of conflicts it allows the publication to be flagged for expert review.

Students reported an average of 15 minutes to review *relevant* publications and five minutes to review *irrelevant* publications. Submissions from second reviewers are automatically stored in our Digital Handbook of χ values.

4.4 Digital Handbook of χ Values

Once a χ value has passed through the review cycle, it is stored in the curated section of the database with associated provenance information that links the value back to the original publication, the item in which it was found, and the reviewers that extracted the value. To facilitate broad access to the database, χDB offers a web service API and HTML website. The website allows users to browse and search the database for specific χ values. The web service API supports ingestion of χ values directly from custom applications, for example to retrieve χ values for a set of specific polymers that may then be used for calculations or visualizations. Both the website and web service are available at http://pppdb.uchicago.edu.

The website allows users to query for information related to a particular polymer. Once the user selects a particular polymer from the search interface, he or she is presented with a table of searchable χ values that relate to that polymer. Each row in the table includes the



POLY(METHYL ACRYLATE)

Flory-Huggins (χ)

Show 10 entries

Search:

	Polymer	χ or χN	A	B	C	T	T unit	Method	DOI
●	poly(ethylene oxide)	-0.04	0.0	0.0	0.0	40.0	C	melting point depression	ma102867d
●	poly(hydroxyethyl acrylate)	0.06	0.0	0.0	0.0	293.0	K	a rheometrics ares-ls1 strain controlled rheometer	ma500905n
●	poly(octyl acrylate)	0.07	0.0	0.0	0.0	293.0	K	a rheometrics ares-ls1 strain controlled rheometer	ma500905n

Figure 3: Screenshot of the χDB Digital Handbook

second compound (polymer or solvent) involved in the interaction, the measurement method used (where available), the temperature at which the parameter was measured (in various forms), and a link to the original publication. Rows can also be expanded to show additional metadata such as molecular masses and concentration. Figure 3 shows an example of χ values for poly(methyl acrylate) in the Digital Handbook.

The χDB REST API supports querying the Digital Handbook for χ values that relate to a specific polymer-polymer or polymer-solvent pair. The REST API has been used to create a Flory-Huggins phase diagram generator for specific polymer blends. This application determines the liquid-liquid curves for a binary blend of polymers, as well as a polymer solution.

5 Results

During the class and over a two month period immediately thereafter, students reviewed 376 publications from the period 2010–2015 in *Macromolecules*. We briefly explore here the results of extractions, looking specifically at the characteristics of the χ values, the range of compounds for which χ values were collected, and the methods used to derive χ values.

χ **Values:** Of the 376 publications reviewed, students deemed 259 (69 %) of the papers *relevant*, of which 145 (38.5 %) of the papers contained one or more χ values. Our dataset includes 388 χ values, including 237 (61 %) polymer-polymer χ values. Measured χ values account for approximately half (48.5 %) of all χ values extracted, the other half (51.6 %) are cited from other publications. Of these measured values, the dataset includes 84 (21.7 %) measured polymer-polymer χ values. In the most focused case of measured polymer-polymer pairs, we found that 70.9 % of χ values were embedded directly in publication text, and 9.7 % in the abstract. Combined, these values indicate that mining text for χ values would potentially capture about 80 % of χ values. The vast majority (89.0 %) of χ values that we identified were published as type 1 or 2 i.e., a number or a linear function of temperature.

Compounds: Polystyrene (PS) is the most studied polymer by a large margin, with 140

χ values collected. The second and third most frequent, Poly(methyl methacrylate) (PMMA) and Polyisoprene (PI), have 59 and 22 χ values, respectively. The average number of χ values per polymer is 4.74. Not surprisingly, the most frequent polymer pair is PS–PMMA, with 36 χ values.

Methods: One final area of great interest to our experts was evaluating the method used to measure the χ values. Unfortunately the method was not always present (or clear) in publications. Students were unable to identify the method for 62 (16.0 %) of the 388 χ values found and were unsure about 12 others (3.1 %), resulting in a total of 19.1 % χ values with no identified method. Originally, experts provided a list of seven methods that they expected would be commonly used. Analysis of our dataset reveals that, for the target case of measured polymer-polymer values these methods are indeed the most commonly used, with only four of the 84 measured polymer-polymer values not using one of these seven methods.

6 Automated Classification

While our approach has established a rich database of χ values, there is potential for further improvements. For example, only 38.5 % of our selected publications contained χ values; thus, about 62 % of the papers curated by reviewers did not in fact contribute to the digital handbook. As a first step towards improving this ratio we have investigated the application of machine learning techniques to optimize the prioritization and classification of *relevant* publications.

To undertake this task, we used the Support Vector Classifier (SVC) from Scikit Learn [11], an open source machine learning Python library. SVC is an implementation of Support Vector Machines (SVMs), supervised learning models with associated learning algorithms that analyze data and recognize patterns. The models map data into a feature space to make predictions.

Three performance metrics are commonly used to evaluate the accuracy of classifiers: precision, recall, and F-measure. Precision and recall are expressed in terms of *Positive* and *Negative* predictions, i.e., in our case *Contains* χ and *Does not contain* χ; *True* and *False* predictions correspond to correct and incorrect predictions. Precision measures the percentage of predictions that were correct while recall measures the percentage of items in the test dataset that were correctly predicted. Precision and recall are defined in Equations 1 and 2.

$$Precision = \frac{TruePositives}{TruePositives + FalsePositives} \tag{1}$$

$$Recall = \frac{TruePositives}{TruePositives + FalseNegatives} \tag{2}$$

The F_X-score is a measure of a test's accuracy. The traditional F-measure or balanced Fscore (F_1 score) is the harmonic mean of precision and recall; it can be interpreted as a weighted average of the precision and recall, with a best value of 1 and worst of 0. The general formula for positive real β is defined in Equation 3.

$$F_\beta = (1+\beta^2) \times \frac{precision \times recall}{\beta^2 .precision + recall} \tag{3}$$

6.1 Test dataset

Our datasets include two sets of abstracts. The first set is composed of all abstracts of publications reviewed by the students, each of which has been classified by them as either *relevant* or *irrelevant*. These 376 publications were selected by the χDB crawler and are therefore biased by the *Flory-Huggins* keyword search. (However, as previously discussed, only 145 of these publications contained χ values.) To address this bias we downloaded an additional 135 publications from two arbitrarily chosen issues of *Macromolecules* (January 12, 2010 and January 26, 2010). Table 1 shows the sets of abstracts used in the classification of abstracts; we call the initial and biased set of abstracts "biased abstracts" and the larger set, which contains both the original 376 biased abstracts and the additional 135 unbiased abstracts, "All abstracts." To classify the additional set of papers we visually inspected the abstracts and full text of each publication and reviewed them for χ values.

Table 1: Characteristics of the abstracts used as input to the classification process

Category	**Biased abstracts**	**Unbiased abstracts**	**All abstracts**
Relevant	145	2	147
Irrelevant	231	133	364
Total	376	135	511

6.2 Results

We applied Scikit Learn's Support Vector Classifier to the set of abstracts, varying just the criteria used to identify abstracts as *relevant* or *irrelevant*. The features used by the classifier are generated using a word-weighting scheme commonly used in information retrieval [13]. The abstracts are first converted to a matrix of token counts and subsequently transformed into a normalized tf-idf (term frequency-inverse document frequency) representation. The two terms are multiplied in order to reduce the impact of terms that occur frequently in a given corpus and thus are less informative. We used three different definitions of *relevancy*: includes χ value; includes measured χ value; and includes measured polymer-polymer χ value.

Table 2 shows that the performance of the classifier for both sets of abstracts. Accuracy improves as *relevancy* becomes more specific. We also see a small (≈3–7 %) improvement in accuracy when using all abstracts. When using all abstracts, the accuracy of classifying measured polymer-polymer relevant papers is 86.9 % precision and 90.9 % recall.

There is a tradeoff between maximizing the number of *relevant* publications (and minimizing the number of *irrelevant* publications) retrieved. Deciding whether these scores are acceptable depends on the cost of errors (false negatives and false positives). Our observed precision score (of 86.9 %) means that 13.1 % *irrelevant* papers remain; a considerable improvement over the initial 61.5 % of publications that did not contain χ values. The recall score of 90.9 % means that we misclassify ≈9 % of *relevant* papers. As ideally we would like to capture all such publications, further work should aim at improving this score. Nevertheless, our results demonstrate the potential of capturing a significant portion of targeted publications in the literature.

We observe that the top 25 features (words) used by our classifier in the most focused case of polymer-polymer pairs include a mixture of more or less χ-related terms. For example, terms like "process," "parameter," and "form" could refer to various experimental settings. On the other hand, the word "domains" (as in microphase domains) is relevant to measuring χ and is also used for a wide variety of applications in which χ is important. χ is a measure of polymer-polymer "interaction" that is present in the list of features. Microphase "morphologies" are relevant to measuring χ via phase diagrams. This combination represents a challenge in further isolating publications that are specifically related to χ and may require incorporating some domain knowledge into the χDB workflow.

Table 2: Classification of abstracts in χDB

Relevancy (contains)	**Metric**	**Biased abstracts**	**All abstracts**
χ Values	Mean F1 score	0.624	0.679
	Mean precision score	60.5 %	65.1 %
	Mean recall score	64.5 %	71.2 %
Measured χ values	Mean F1 score	0.790	0.835
	Mean precision score	75.9 %	80.9 %
	Mean recall score	82.2 %	86.4 %
Measured polymer-polymer χ values	Mean F1 score	0.852	0.890
	Mean precision score	82.7 %	86.9 %
	Mean recall score	87.8 %	90.9 %

7 Conclusion and Future Work

As part of a long-term project to create a digital handbook of polymer properties, we have developed χDB, a hybrid human computer-system that extracts the Flory-Huggins (or χ) parameter from scientific literature. Our work to date has extracted 388 χ values for 120 polymers and 30 solvents. Our 237 measured χ values for blends of 63 unique polymers exceed the 134 χ values for blends of 41 unique polymers found in the *Physical Properties of Polymers Handbook* [7]. One reason for our superior performance is that we were able to collect values reported after the 2007 publication of the *Handbook* (84 of our χ values are from 2010 to 2015); another is that our more exhaustive search leads us to find earlier values not reported in the *Handbook*. Our results emphasize the potential for using our approach to create and maintain a digital database of χ parameters that is more comprehensive and up to date than any survey publication. The database is currently available at http://pppdb.uchicago.edu.

Using publications marked *relevant* and machine learning software, we were able to improve the publication selection process considerably, decreasing the number of reviewed publications that do not contribute to the χ database from 61.5 % to 13.1 %. We hope in future work to further improve this classification process by using alternative methods and by integrating polymer science insight gained through exploration of our data collection. For example, we will explore the utility of using more frequently occurring methods as a publication filter prior to running the classifier. We are exploring collaborations with journals in order to gain access to more publications and mine more properties. While this work is focused on χ, the steps required to collect a new property are straightforward; first the crawler must be configured to use a different keyword; the schema for the target property will guide the design of a new input form and the corresponding database table. Future work will also involve addressing crowdsourcing challenges in order to recruit more trained users and experts. Scaling out χDB will also lead us to explore deep learning systems for fact extraction [16].

Acknowledgments

We thank the student contributors to χDB. This work was supported in part by NIST contract 60NANB15D077, the Center for Hierarchical Materials Design, and DOE contract DE-AC02-06CH11357. Certain commercial equipment and/or materials are identified in this report in order to adequately specify the experimental procedure. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology,

nor does it imply that the equipment and/or materials used are necessarily the best available for the purpose.

References

[1] M. Banko, M. J. Cafarella, S. Soderland, M. Broadhead, and O. Etzioni. Open information extraction for the web. In *Proceedings of the 20th International Joint Conference on Artifical Intelligence (IJCAI)*, pages 2670–2676, 2007.

[2] D. A. Benson, I. Karsch-Mizrachi, D. J Lipman, J. Ostell, B. A Rapp, and D. L. Wheeler. Genbank. *Nucleic Acids Research*, 28(1):15–18, 2000.

[3] M. Buhrmester, T. Kwang, and S. D. Gosling. Amazon's Mechanical Turk A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, 6(1):3–5, 2011.

[4] Erik Cambria and Bruce White. Jumping nlp curves: a review of natural language processing research [review article]. *Computational Intelligence Magazine, IEEE*, 9(2):48–57, 2014.

[5] J. Cowie and W. Lehnert. Information extraction. *Communications of the ACM*, 39(1):80–91, 1996.

[6] J. J. de Pablo, B. Jones, C. L. Kovacs, V. Ozolins, and A. P. Ramirez. The Materials Genome Initiative, the interplay of experiment, theory and computation. *Current Opinion in Solid State and Materials Science*, 18(2):99–117, 2014.

[7] H. B. Eitouni and N P. Balsara. Thermodynamics of polymer blends. In *Physical Properties of Polymers Handbook*, pages 339–356. Springer, 2007.

[8] A. Jain, S. Ping Ong, G. Hautier, W. Chen, W. D. Richards, S. Dacek, S. Cholia, D. Gunter, D. Skinner, and G. Ceder. Commentary: The Materials Project: A materials genome approach to accelerating materials innovation. *APL Materials*, 1(1):011002, 2013.

[9] M. D. Mailman, M. Feolo, Y. Jin, M. Kimura, K. Tryka, R. Bagoutdinov, L. Hao, A. Kiang, J. Paschall, L. Phan, et al. The NCBI dbGaP database of genotypes and phenotypes. *Nature Genetics*, 39(10):1181–1186, 2007.

[10] I. Muslea. Extraction patterns for information extraction tasks: A survey. In *The AAAI-99 Workshop on Machine Learning for Information Extraction*, pages 1–6, 1999.

[11] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12:2825–2830, 2011.

[12] M. J. Raddick, G. Bracey, P. L. Gay, C. J. Lintott, C. Cardamone, P. Murray, K. Schawinski, A. S. Szalay, and J. Vandenberg. Galaxy Zoo: Motivations of citizen scientists. *arXiv preprint arXiv:1303.6886*, 2013.

[13] Juan Ramos. Using tf-idf to determine word relevance in document queries. In *Proceedings of the first instructional conference on machine learning*, 2003.

[14] A. Rzhetsky, I. Iossifov, T. Koike, M. Krauthammer, P. Kra, M. Morris, H. Yu, P. A. Duboué, W. Weng, W. J. Wilbur, Hatzivassiloglou V., and C. Friedman. GeneWays: A system for extracting, analyzing, visualizing, and integrating molecular pathway data. *Journal of Biomedical Informatics*, 37(1):43–53, 2004.

[15] C. Seifert, M. Granitzer, P. Höfler, B. Mutlu, V. Sabol, K. Schlegel, S. Bayerl, F. Stegmaier, S. Zwicklbauer, and R. Kern. Crowdsourcing fact extraction from scientific literature. In *Human-Computer Interaction and Knowledge Discovery in Complex, Unstructured, Big Data*, pages 160–172. Springer, 2013.

[16] J. Shin, S. Wu, F. Wang, C. De Sa, C. Zhang, and C. Ré. Incremental knowledge base construction using Deepdive. *Proceedings of the VLDB Endowment*, 8(11):1310–1321, 2015.

[17] PJ Spencer. A brief history of CALPHAD. *Calphad*, 32(1):1–8, 2008.

[18] Dirk Willem Van Krevelen and Klaas Te Nijenhuis. *Properties of polymers: their correlation with chemical structure; their numerical estimation and prediction from additive group contributions.* Elsevier, 2009.

[19] M. Ware and M. Mabe. The STM report: An overview of scientific and scholarly journal publishing. Technical report, STM, 2009.

An Investigation to Manufacturing Analytical Services Composition using the Analytical Target Cascading Method

Kai-wen Tien[1], Boonserm Kulvatunyou[2], Kiwook Jung[2], and Vittaldas Prabhu[1]

[1]Penn State University, State College, PA, U.S.A.
kut147@psu.edu, vxp7@engr.psu.edu
[2]National Institute of Standards and Technology, Gaithersburg, MD, U.S.A.
{serm, kiwook.jung}@nist.gov

Abstract. As cloud computing is increasingly adopted, the trend is to offer software functions as modular services and compose them into larger, more meaningful ones. The trend is attractive to analytical problems in the manufacturing system design and performance improvement domain because 1) finding a global optimization for the system is a complex problem; and 2) sub-problems are typically compartmentalized by the organizational structure. However, solving sub-problems by independent services can result in a sub-optimal solution at the system level. This paper investigates the technique called Analytical Target Cascading (ATC) to coordinate the optimization of loosely-coupled sub-problems, each may be modularly formulated by differing departments and be solved by modular analytical services. The result demonstrates that ATC is a promising method in that it offers system-level optimal solutions that can scale up by exploiting distributed and modular executions while allowing easier management of the problem formulation.

Keywords: factory design and improvement, integration optimization, analytical target cascading, smart manufacturing, services composition

1 Introduction

As cloud computing is increasingly adopted, the trend is to offer software functions, including analytical software functions, as modular services and compose them into larger, more meaningful ones [1, 2]. The trend is attractive to analytical problems in the manufacturing system design and performance improvement domain because 1) finding a global optimization for the system is a complex problem; and 2) sub-problems are typically compartmentalized by the organizational structure. However, solving sub-problems independently can result in a sub-optimal solution at the system level.

This paper investigates the technique called Analytical Target Cascading (ATC) to coordinate the optimization of loosely-coupled sub-problems. Each sub-problem may be independently formulated by each stake-holding organization and be solved by modular analytical software services.

adfa, p. 1, 2011.
© Springer-Verlag Berlin Heidelberg 2011

SP-972
Tien, Kai-wen; Kulvatunyou, Boonserm; Jung, Kiwook; Prabhu, Vittaldas.
"An Investigation to Manufacturing Analytical Services Composition using the Analytical Target Cascading Method."
Paper presented at the APMS International Conference, Advances in Production Management Systems, Iguassu Falls, Brazil, Sep 3-Sep 7, 2016.

This study is motivated by the Factory Design and Improvement reference activity model developed in [4]. The model decomposes major activities into subtasks and key decision-makings needed in a typical factory design and performance improvement project. It entails the needs for interactions across optimization problems at multiple control-levels.

For simplification of the illustration, this paper investigated the ability of ATC to coordinate three sub-problems at the manufacturing process control level including capacity design, lot sizing, and storage layout design. These three sub-problems are interlinked and typically dealt by different stakeholders. Their linkages are shown in Fig. 1.

Many analytical techniques have been developed to solve each of these three sub-problems. These techniques are often used in isolation, but these problems are not independent. A change in one formulation can influence the outcomes and feasibilities of the other two. Therefore, capturing those dependencies and using them to integrate these three sub-problems is crucial.

ATC has been used to solve multidisciplinary-design-optimization problems that comprise heterogeneous sub-problems. These sub-problems are solved separately; but, each of their interim solutions is communicated regularly. This not only speeds convergence, it also gives a better solution than the one that is generated with no communication or one-way communication (such as in the hierarchical model in Fig. 1). The algorithm that ATC uses has been studied extensively and its convergence properties have been established mathematically [5]. The primary application of ATC has been in designing complex products such as automobiles and aircrafts [6, 7]. Nevertheless, it has also been used in integrating supply chains and integrating marketing and production (DFM) [8, 9].

The result of this investigation indicates that ATC is a promising method in that it offers (1) easier management of the problem formulation of the overall system and (2) coherent, optimal solutions that can scale up to the size of the overall system by exploiting distributed and modular executions.

The rest of the paper is organized as follow. In Section 2, the analytical sub-problems are introduced; and it discusses drawbacks of the two traditional integration structures to compose these sub-problems: centralized and hierarchical. Then, the mathematical formulation of the proposed ATC-based collaborative structure illustrated in Fig. 1(c), is described in Section 3. In Section 4, we apply ATC to the sub-problems and analyze the results using data from a production project at Penn State [10]. Finally, the conclusion is presented in Section 5.

2 Composing Manufacturing Analytical Models

In this section, we introduce the three optimization sub-problems and their corresponding links. The exact links depend on the multi-criteria optimization of throughput (TH), inventory (INV), and work-in-process (WIP). Links can be seen as either common decision variables or input/output parameters, which are assumed to be non-negative.

Note: $\pi(\cdot)$ is a penalty function which is used in the collaborative model and will be explained in section 3.1. In this section, we set it as a zero function.

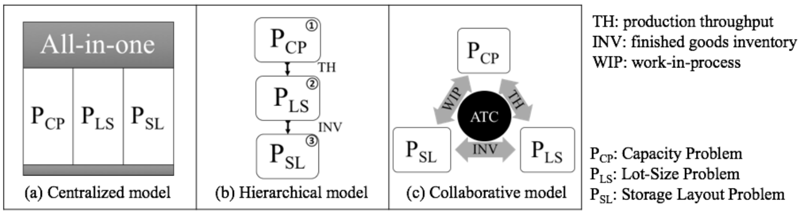


Fig. 1. Integration models of analytical sub-problems

2.1 Capacity Optimization

The important concern when optimizing capacity is that cycle times and WIP levels grow dramatically with increasing utilization [11]. Thus, the designers of this activity should decide on a reasonable throughput which minimizes the average WIP.

($\mathrm{P_{CP}}$)

$$\min\ z_1(\mathrm{TH},\mathrm{WIP}) = c_w\cdot\mathrm{WIP} + \pi(\mathrm{TH},\mathrm{WIP})$$

$$s.t.\quad \mathrm{CT_q} = \frac{c_a^2+c_e^2}{2}\cdot\frac{u}{1-u}\cdot t_e \qquad (1\text{-}1)$$

$$\mathrm{WIP} = \mathrm{TH}\cdot\mathrm{CT_q} \qquad (1\text{-}2)$$

$$u = \mathrm{TH}\cdot t_e \qquad (1\text{-}3)$$

$$TH \leq \mathrm{TH_{limit}} \qquad (1\text{-}4)$$

where c_w is the unit cost for holding one unit of WIP during the planning period, and π represents any penalty functions. Equation (1-1) represents the approximation of the waiting time in queue, $\mathrm{CT_q}$, in a G/G/1 system. The formulation shows that $\mathrm{CT_q}$ is effected by the coefficient of variation (CV) of inter-arrival times c_a, the CV of effective processing times c_e, the utilization u, and the effective process time t_e. The formulation can be generalized to multi-machine, multi-station systems. (1-2) represents the Little's law formula. (1-3) shows the equation of utilization and (1-4) restricts TH.

2.2 Lot-Sizing Optimization

A wealth of models can be used for making lot-size decisions including EOQ (Economic Order Quantity) and EPL (Economic Production Lots) [11]. Here, we minimize the total inventory cost over T periods.

($\mathrm{P_{LS}}$)

$$\min\ z_2(\mathrm{TH},\mathrm{INV}) = \sum_{t=1}^{T} p_t x_t + h_t i_t + \pi(\mathrm{TH},\mathrm{INV})$$

$$s.t.\quad i_t = x_t + i_{t-1} - D_t,\quad \forall t = 1\ldots T \qquad (2\text{-}1)$$

$$x_t \leq \mathrm{TH}\cdot\mathrm{WH},\qquad \forall t = 1\ldots T \qquad (2\text{-}2)$$

$$x_t + i_{t-1} \leq \mathrm{INV},\qquad \forall t = 1\ldots T \qquad (2\text{-}3)$$

where p_t is the unit production cost and h_t is the unit holding cost for period t. Equation (2-1) shows the inventory balance in each period, in which D_t is the demand and x_t is the production amount in period t. The constraint (2-2) indicates the production amount should be less than capacity limit, in which WH is the available working hours during the period. Equation (2-3) shows the inventory level should be less than INV.

2.3 Storage Layout Optimization

The storage layout sub-problem determines the optimal layout to minimize the material handling costs in terms of the distances 1) from WIP storage locations to locations of machines, and 2) between finished-goods inventory locations to the shipping docks. The storage layout problem is usually formulated as an assignment problem in which the storage floor is first subdivided into N grid squares and each item (WIP or INV) is assigned to a grid square.

$$(\mathrm{P_{SL}}) \quad \min\ z_3(\mathrm{INV}, \mathrm{WIP}) = \sum_{k=1}^{N}[c_k^{(w)} y_k^{(w)} + c_k^{(f)} y_k^{(f)}] + \pi(\mathrm{INV}, \mathrm{WIP})$$

$$s.t. \quad \sum_{k=1}^{N} y_k^{(w)} \geq \mathrm{WIP} \qquad (3\text{-}1)$$

$$\sum_{k=1}^{N} y_k^{(f)} \geq \mathrm{INV} \qquad (3\text{-}2)$$

$$\mathrm{y}_{\mathrm{j}}^{(w)} + y_j^{(f)} \leq 1, \qquad \forall\, j = 1,2, \dots, N \qquad (3\text{-}3)$$

$$y_k^{(w)}, y_k^{(f)} \in \{0, 1\} \qquad (3\text{-}4)$$

where $c_k^{(w)}$ and $c_k^{(f)}$ are the material handling cost for respectively storing one work-in-process and inventory in the grid square k. $y_k^{(w)}$ $(y_k^{(f)})$ is a binary decision variable, which value is 1 if one unit of WIP (INV) is assigned to the grid square k. (3-1) and (3-2) represent the storage spaces demanded for WIP and INV, respectively. (3-3) restricts that one grid square can store only one unit of the items.

2.4 Centralized vs. Hierarchical Integration Structures

The centralized-structure approach, shown as Fig. 1(a), is an intuitive and coherent way to think about integrating the sub-problems. It results from minimizing the three objective functions of the sub-problems subject to all constraints (1-1) to (3-4). So, in essence there is only one, multi-objective function and one set of constraints. There are, however, two serious drawbacks associated with this centralized approach. First, is the issue of poor scalability of the approach in terms of the increasing number of decision variables and constraints. The other drawback occurs when reformulation of the model is needed, e.g., when the factory changes: essentially you basically have to start over.

The hierarchical-structure approach, shown in Fig. 1(b), reduces, but does not eliminate, the difficulty in addressing these two challenges. The sub-problems are solved individually, so reformulation is easier. Additionally, the sub-problems are typically solved in a prescribed order. That order is P_{CP}, P_{LS}, then P_{SL} [4]. The links are directed links and are obtained as the outputs of the previously solved sub-problems. Clearly, this approach is not guaranteed to find a coherent, optimal solution. In addition, the quality of the final solution is highly dependent on the initial inputs to the initial process, P_{CP}. Therefore, in practice, it requires many experiments, by varying the input conditions until an optimal solution is found across all the sub-problems!

3 Proposed Collaborative Approach

Our collaborative approach achieves both the high solution quality of the centralized approach as well as the re-configurability of the hierarchical approach. The ATC algorithm connects sub-problems as if they were building-blocks. First, sub-problems at two ends of a link are assigned two specific roles: sender or receiver. Then, the link value in each sub-problem is replaced by two variables: target t_i and response r_i. The sender solves the target t_i and the receiver solves the response variable r_i within its own local variables and constraints. The ATC algorithm seeks to minimize the discrepancies between targets and responses with respect to the links. In this paper, as we said above, P_{CP} is the sender of both WIP and TH; P_{LS} is the receiver of TH and the sender of INV; and P_{SL} is the receiver of both WIP and INV as Fig. 1(c).

3.1 The Collaboration strategy

In order to achieve global consistency, each of the three sub-problems is assigned a different penalty function. It "punishes" a sub-problem, by adding high costs to its objective function, when its solution violates consistency constraints. Realizing this, we decided to use the augmented Lagrangian as our penalty function and the basis for our collaboration strategy [12]. The penalty function is shown in equation (4). Note that the notation "∘" means the elementwise product for arrays.

$$\pi(\cdot) = \sum_{i=1}^{n_t}(v_i t_i + \|w_i \circ (t_i - \overline{r_i})\|_2^2) + \sum_{j=1}^{n_r}(-v_j r_j + \|w_j \circ (\overline{t_j} - r_j)\|_2^2) \qquad (4)$$

The Lagrangian penalty function includes two new variables, Lagrangian multiplier v_i and quadratic penalty weight w_i. They are updated in the outer loop of ATC. The updating methods are expressed below, where l represents the iteration of the ATC algorithm.

$$v_i(l+1) = v_i(l) + w_i(l) \circ w_i(l) \circ (t_i(l) - r_i(l)) \qquad (5)$$
$$w_i(l+1) = \beta \circ w_i(l) \qquad (6)$$

The ATC algorithm has three main steps:

Step 1: Inner loop – solving sub-problems separately and updating the target and response variables.

Step 2: Outer loop – updating the Lagrangian multipliers and weights via expression (5) and (6).

Step 3: Termination – terminating the algorithm when the discrepancies of all target and response pairs are smaller than a given tolerance.

3.2 Reconfigurability and Discrepancy Visualization

As mentioned in the previous section, the ATC algorithm connects the sub-problems through target and response variables. It has the advantage of reusability. Suppose, for instance, a company wants to replace their current EOQ sub-problem with a (Q, r) sub-problem for lot-sizing design; the other two sub-problems are still reusable. Furthermore, since the overall system-problem has been partitioned into three sub-problems, the structural complexity of the overall system is reduced. Stakeholders of each sub-problem can also formulate their problems independently; therefore, the factory design and performance improve project can progress efficiently.

The ATC approach also allows feasibility issues across sub-problems to be conveniently resolved. It monitors the target/response values and showing the discrepancies between differing objectives in sub-models. For example, if there was a space reduction made in P_{SL} problem causing the responses r_{WIP} and r_{INV} not meeting the targets given by the other two sub-problems. The discrepancy can be shown in the results. This allows for the stakeholders to effectively collaborate and resolve the specific conflict.

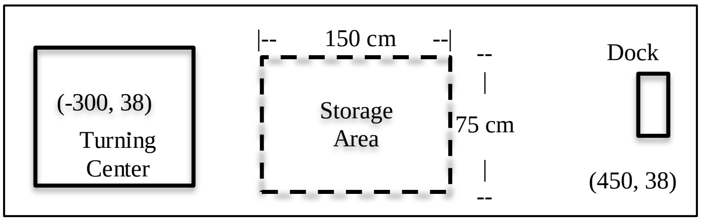


Fig. 2. Factory layout

4 Case Study

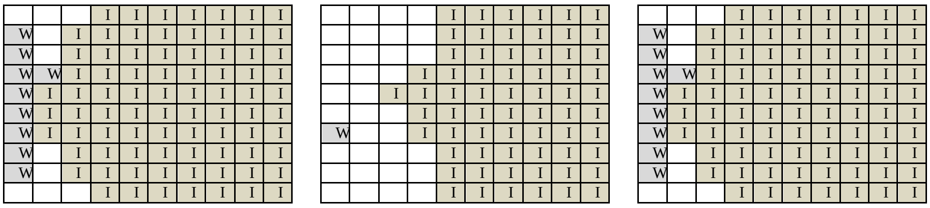
We use the IME Inc. project [10] to demonstrate the potential benefits of our collaborative approach over the other two. The aluminum chess set is the primary product in this case study. The associated process plan includes only one turning center and 240 labor hours. In addition, the product will be delivered to customers at the end of each quarter (March 31th, June 30th, etc.). Note, this knowledge could be used to determine the minimum value for storage size. That minimum value has to be large enough to store both WIPs and finished products during that time. Table 1 shows the parameters for the design sub-problems. c_a is approximated by the variance of the demand and c_e is significant because of the long set-up time of this product. t_e represents the effective processing time for the whole chess set. The production costs p_t changes because of the fluctuation of material costs. The holding cost for one set per one week is estimated by the typical interest rate per quarter (about 6.25%) times the production costs. The factory has 150×75 (cm^2) area for both WIP and the finished products (see Fig. 2). A finished product is wrapped into a 15×7.5×7.5 (cm^3) box. Moreover, the boxes cannot be piled up because of the strength of the boxes. Hence, the storage area is divided into a grid of 100 squares, each of which can store only one box or one working-in-process. The material handling cost of a finished product at a certain location is calculated by multiplying the unit operation cost with the rectangular distance between the machine and the exit dock. With a technician's suggestion, we assume the unit costs of the material handling costs is \$0.01/2.5 centimeter.

Table 1. The parameters of sub-problems

P_{CP} Sub-problem		P_{LS} Sub-problem (Quarterly Plan)		P_{SL} Sub-problem	
c_a	0.685	p_t(\$/sets)	(20.0, 25.0, 18.0, 20.0)	Area (cm^2)	(150, 75)
c_e	0.942	h_t(\$/sets)	(1.25, 1.56, 1.13, 1.25)	Box (cm^2)	(15, 7.5)
t_e(hrs)	1.388	D_t(sets)	(100, 80, 130, 90)	Unit cost (\$/cm)	0.01
c_w(\$)	4	WH(hrs)	240		

Table 2. The Computational Results

	Centralized model	Hierarchical model	Collaborative model
Comp Time (sec)	4.9176	0.0742	132.7390
Total Cost (\$)	8290.5	8388.4	8290.5
(TH_0, WIP_0, INV_0)	(0.43, 0, 0)	(0.43, 0, 0)	(0.43, 0, 0)
(TH*, WIP*, INV*)	(0.67,7.80,80.01)	(0.43,0.54,62.5)	(0.67,7.80,80.01)



			I	I	I	I	I	I	I
W		I	I	I	I	I	I	I	I
W		I	I	I	I	I	I	I	I
W	W	I	I	I	I	I	I	I	I
W	I	I	I	I	I	I	I	I	I
W	I	I	I	I	I	I	I	I	I
W	I	I	I	I	I	I	I	I	I
W		I	I	I	I	I	I	I	I
W		I	I	I	I	I	I	I	I
			I	I	I	I	I	I	I

(a) Centralized model

				I	I	I	I	I	I
				I	I	I	I	I	I
				I	I	I	I	I	I
			I	I	I	I	I	I	I
		I	I	I	I	I	I	I	I
			I	I	I	I	I	I	I
W			I	I	I	I	I	I	I
				I	I	I	I	I	I
				I	I	I	I	I	I
				I	I	I	I	I	I

(b) Hierarchical model

			I	I	I	I	I	I	I
W		I	I	I	I	I	I	I	I
W		I	I	I	I	I	I	I	I
W	W	I	I	I	I	I	I	I	I
W	I	I	I	I	I	I	I	I	I
W	I	I	I	I	I	I	I	I	I
W	I	I	I	I	I	I	I	I	I
W		I	I	I	I	I	I	I	I
W		I	I	I	I	I	I	I	I
			I	I	I	I	I	I	I

(c) Collaborative model

Fig. 3. The storage layouts

The desired throughput (initial value) is determined by the average demand rate 0.43 sets/hr. The three models were constructed and run in MATLAB 2015a. The collaborative model was terminated after 96 iterations, resulting in a tolerance value of 10E-6 for the discrepancies between sub-problems. When terminated, $w =$ (1, 1, 1) and $v =$ (-3.75, 1.34, 1.76). The results show that the proposed collaborative approach can find the same solution as overall optimal solution generated by the centralized approach, but the hierarchical approach cannot. However, the computation time of the collaborative model is much larger than those of the other two (less than 5 seconds). This implies that the collaborative model is more suitable for solving problems in the factory "design stage," where the system complexity issue is much more critical than the computational time. Nevertheless, a parallel computing model could be explored to speed up the solver to provide a solution in a near real-time.

5 Conclusion

In this paper, we proposed a collaborative approach, called Analytical Target Cascading (ATC), to composing analytical sub-problems and possibly associated software services to meet the overall objective. Our experiment shows a promising result. Sub-problems can be formulated and executed modularly and possibly under a distributed computing scheme. Even so, ATC connects these sub-problems and has the capability to achieve the coherent optimal as in the centralized model. Furthermore, unlike the centralized approach, our approach allows sub-problems to be changed or improved easily. Moreover, the discrepancies between targets and responses in each sub-problem are visible allowing for feasibility issues to be easily resolved. In the future work, we are planning to integrate control-level problems and design-level problems.

Acknowledgement: The work described in this paper was funded in part by NIST cooperative agreement with Penn State University No. 70NANB14H255.

Disclaimer: Any mention of commercial products is for information only; it does not imply recommendation or endorsement by NIST.

Reference

1. Kulvatunyou B., et al. On architecting and composing engineering information services to enable smart manufacturing. J. of Computing and Information Science in Egineering (2016).
2. IBM Watson Developer Cloud. Internet Web Site. Accessed May 11, 2016. Available at https://www.ibm.com/smarterplanet/us/en/ibmwatson/developercloud/.
3. Kang, H., et al. Smart manufacturing: Past research, present findings, and future directions. Intl J. of Precision Engineering and Manufacturing-Green Technology. 3, 111-128 (2016).
4. Choi, S., et al. A diagnosis and evaluation method for strategic planning and systematic design of a virtual factory in smart manufacturing systems. Intl. J. of Precision Engineering and Manufacturing. 16, 1107-1115 (2015).
5. Michelena, N., et al. Convergence Properties of Analytical Target Cascading. AIAA Journal. 41, 897-905 (2003).
6. Kim, H., et al. Analytical Target Cascading in Automotive Vehicle Design. J. of Mechanical Design. 125, 481 (2003).
7. Allison, J., et al. Analytical target cascading in aircraft design. In 44th AIAA aerospace sciences meeting and exhibit. 9-12 (2006).
8. Qu, T., et al. Optimal configuration of assembly supply chains using analytical target cascading. Intl. J. of Production Research. 48, 6883-6907 (2010).
9. Michalek, J., et al. Balancing Marketing and Manufacturing Objectives in Product Line Design. J. of Mechanical Design. 128, 1196 (2006).
10. FAME LAB, http://www.engr.psu.edu/cim/FAME/CIMLAB/cim_p_2000.html
11. Hopp, W. & Spearman, M. L.: Factory physics. Waveland Press, (2011)
12. Tosserams, S., et al. A Nonhierarchical Formulation of Analytical Target Cascading. J. of Mechanical Design. 132, 051002 (2010).

Proceedings of the ASME 2016 International Manufacturing Science and Engineering Conference
MSEC2016
June 27-July 1, 2016, Blacksburg, Virginia, USA

MSEC2016-8792

GAPS ANALYSIS OF INTEGRATING PRODUCT DESIGN, MANUFACTURING, AND QUALITY DATA IN THE SUPPLY CHAIN USING MODEL-BASED DEFINITION

Asa Trainer
International TechneGroup Incorporated
Milford, Ohio

Thomas Hedberg, Jr.
National Institute of Standards and Technology
Gaithersburg, Maryland

Allison Barnard Feeney
National Institute of Standards and Technology
Gaithersburg, Maryland

Kevin Fischer
Rockwell Collins
Cedar Rapids, Iowa

Phil Rosche
Advanced Collaboration Consulting Resources
Summerville, South Carolina

KEYWORDS

Model-based definition, product lifecycle management, digital manufacturing, product data verification and validation

ABSTRACT

Advances in information technology triggered a digital revolution that holds promise of reduced costs, improved productivity, and higher quality. To ride this wave of innovation, manufacturing enterprises are changing how product definitions are communicated – from paper to models. To achieve industry's vision of the Model-Based Enterprise (MBE), the MBE strategy must include model-based data interoperability from design to manufacturing and quality in the supply chain. The Model-Based Definition (MBD) is created by the original equipment manufacturer (OEM) using Computer-Aided Design (CAD) tools. This information is then shared with the supplier so that they can manufacture and inspect the physical parts. Today, suppliers predominantly use Computer-Aided Manufacturing (CAM) and Coordinate Measuring Machine (CMM) models for these tasks. Traditionally, the OEM has provided design data to the supplier in the form of two-dimensional (2D) drawings, but may also include a three-dimensional (3D)-shape-geometry model, often in a standards-based format such as ISO 10303-203:2011 (STEP AP203). The supplier then creates the respective CAM and CMM models and machine programs to produce and inspect the parts. In the MBE vision for model-based data exchange, the CAD model must include product-and-manufacturing information (PMI) in addition to the shape geometry. Today's CAD tools can generate models with embedded PMI. And, with the emergence of STEP AP242, a standards-based model with embedded PMI can now be shared downstream.

The on-going research detailed in this paper seeks to investigate three concepts. First, that the ability to utilize a STEP AP242 model with embedded PMI for CAD-to-CAM and CAD-to-CMM data exchange is possible and valuable to the overall goal of a more efficient process. Second, the research identifies gaps in tools, standards, and processes that inhibit industry's ability to cost-effectively achieve model-based-data interoperability in the pursuit of the MBE vision. Finally, it also seeks to explore the interaction between CAD and CMM processes and determine if the concept of feedback from CAM and CMM back to CAD is feasible. The main goal of our study is to test the hypothesis that model-based-data interoperability from CAD-to-CAM and CAD-to-CMM is feasible through standards-based integration. This paper presents several barriers to model-based-data interoperability. Overall, the project team demonstrated the exchange of product definition data between CAD, CAM, and CMM systems using standards-based methods. While gaps in standards coverage were identified, the gaps should not stop industry's progress toward MBE. The results of our study provide evidence in support of an open-standards method to model-based-data interoperability, which would provide maximum value and impact to industry.

INTRODUCTION

Information technology advances such as big data, service-oriented architectures, and networking have triggered a digital revolution [1] that holds promise of reduced costs, improved productivity, and higher quality. Modern manufacturing

This work is in part a work of the U.S. Government. ASME disclaims all interest in the U.S. Government's contributions.

enterprises are both more globally distributed and digital than ever before, resulting in increasingly complex manufacturing system networks [2, 3]. Manufacturers are under mounting pressure to perform digital manufacturing more efficiently and effectively within these distributed manufacturing systems. To do so, industry is changing how product definitions are communicated – from paper to models. The transition to model-based enterprise (MBE) has introduced new requirements on data usage in the manufacturing systems. The need for automated methods to collect, transmit, analyze, and act on the most appropriate data is gaining attention in the literature [4-7]. In addition, the MBE strategy must ensure model-based-data interoperability between design activities (e.g., product and assembly design) and manufacturing activities (e.g., fabrication, assembly, and quality assurance).

Tool developers of model-based data exchange have primarily focused on computer-aided design (CAD)-to-CAD data interoperability and long-term data archival. While computer-aided manufacturing (CAM) and (coordinate measurement machine (CMM) systems[1] can also ingest model-geometry data and product-and-manufacturing information (PMI) through their respective application program interfaces (APIs), they do so through vendor-specific formats.

A team of Aerospace and Defense industry sector members, software solution providers, and researchers from the National Institute of Standards and Technology (NIST) conducted a study of model-based-data interoperability across the product lifecycle – focusing on design, manufacturing, and inspection.

Our objective was to test the hypothesis that model-based-data interoperability from CAD-to-CAM and CAD-to-CMM is feasible through standards-based integration.

The project team used the recently published STandard for the Exchange of Product (STEP) model data, ISO 10303-242:2014 [8] titled “Managed Model Based 3D Engineering,” or STEP AP242, as our standards-based format exported from the CAD system. Many CAM and CMM solution providers use either the ACIS or Parasolid geometric-modeling kernels, so the project team considered these geometric-modeling kernels to be defacto standards. In the research, the project team translated native 3D-CAD models with PMI to the STEP AP242 standards-based format and exchanged the validated translations with a Parasolid-based CAM system and ACIS-based CMM system.

Now, with the introduction of STEP AP242, the project team asked if industry has the tools it needs to move toward the MBE vision. Can industry achieve a vision that includes model-based-data interoperability when going from design to manufacturing and inspection across the supply chain?

The project team identified, in our study, several barriers to model-based-data interoperability. The first barrier is that the majority of industry still considers the two-dimensional (2D) drawing the legal master data record, versus the three-dimensional (3D) model. There is also a significant learning curve for data authors to effectively enrich a 3D-CAD model with the 3D annotations and data that are needed to support downstream processes. Also, in the context of automation, many APIs do not adequately support reading and writing of standards-based PMI. In addition, easy data exchange through standards-based implementations threatens to upend the business model of major product-lifecycle management (PLM) tools. Lastly, the CAM and CMM markets are distributed across many small-to-medium enterprise (SME) manufacturers, which lack industry’s ability to drive CAM and CMM solution providers to implement standards-based solutions.

BACKGROUND

In the United States, the manufacturing supply base consists significantly of SME manufacturers. Today, suppliers predominantly use CAM and CMM models to conduct manufacturing and inspection activities. An OEM typically sends the product definition to suppliers in the form of full-detail 2D drawings, which are in most cases the legal master data form. Thus, suppliers spend considerable time converting 2D product-definition data back to usable 3D product definition. Research supports the business case and benefits of MBE [9]. The widespread adoption of MBE would eliminate these manual conversions, which are time consuming and may introduce error.

More recently, the product-definition data delivered to suppliers also includes a 3D-shape-geometry model. This shape-geometry model is often provided in a standards-based format, typically ISO 10303-214:2010 (STEP AP214) [10] and ISO 10303-203:2011 (STEP AP203) [11]. However, in addition to shape geometry, the CAM and CMM processes require additional, non-geometric information (PMI) to fabricate and inspect the part. This information may be presented for human consumption in the STEP AP203 exchange, but it is not available in a computer-processable form.

MBE strategy must include model-based-data interoperability for design to manufacturing and quality in the supply chain. In MBE, data authors use computer-aided-design (CAD) tools to create a model-based definition (MBD). A MBD is a 3D digital-product model that defines the requirements and specifications of the product – including computer-processable PMI in the form of 3D annotations and data. Figure 1 presents an example of a MBD. After releasing the MBD, an original-equipment manufacturer (OEM) sends the MBD to a supplier to manufacture and inspect the physical parts.

Despite the industry MBE vision to become model-based, there is still a reliance on 2D drawings. A survey [12] of SME suppliers showed that many of those surveyed still receive design data from their OEM customers in the form of full-detail-2D drawings. Another large group receives a 3D-shape-geometry model combined with a 2D drawing containing the PMI. Only a small percentage of the SME manufacturers

[1] NOTE: The term “Coordinate Measurement System” (CMS) is gaining in popularity to describe the evolution of the metrology domain towards an integrated system of both coordinate measurement software and hardware.

receive just a 3D model with embedded PMI. The design to manufacturing process is still very much drawing-based. The few data exchanges that are model-based with embedded PMI use proprietary, not standards-based, models [13].

A widely used standard format is STEP. Its development started in 1984 with the objective to provide a mechanism that is capable of describing product data throughout the life cycle of a product, independent from any particular system. The nature of this description makes it suitable not only for neutral file exchange, but also as a basis for implementing and sharing product databases and archiving [14].

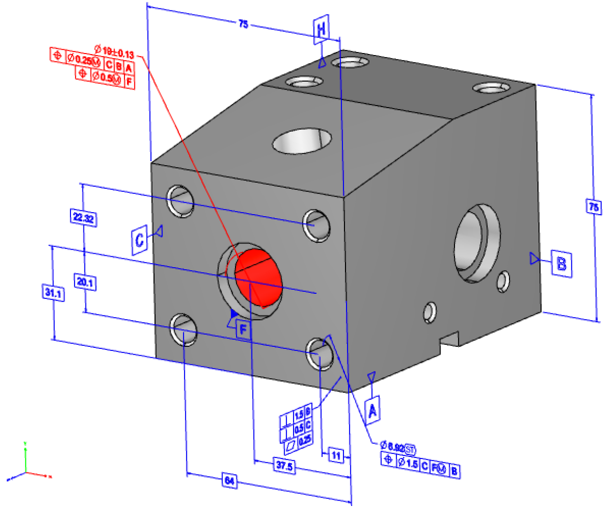


Figure 1: Example model-based definition

STEP includes a series of integrated data models known as application protocols (APs). There are dozens of STEP APs, which fall into the three main areas – design, manufacturing, and lifecycle support.

Today, both STEP AP203 and AP214 are still one of the most important parts of ISO 10303. Many CAD systems support STEP AP203 and AP214 for importing and exporting data. According to another survey [12] of SME manufacturers, STEP AP203 is the most commonly used format for CAD-to-CAD data interoperability. However, the STEP AP203 model contains only shape geometry, and not the PMI necessary for downstream processes.

In December 2014, the International Standards Organization (ISO) published the first edition of the application protocol STEP AP242, which combined and replaced several APs related to the presentation and representation of product-definition data. In addition, STEP AP242 contains extensions and significant updates for dimensional and geometric tolerances, kinematics, and tessellation. In other words, STEP AP242 offers standards-based models that include the representation of PMI that is computer interpretable [15]. This is a major breakthrough that supports manufacturing's need for model-based CAM and CMM processes.

While standards-based exchange provides significant benefit to industry, one challenge that must be addressed is verification and validation of translations, ensuring adequate product-data quality. The need for confidence in the conformance of 3D model data to quality standards is well understood [16]. Requirements for verification of model data, particularly PMI data, and validation of derivative variants of that data for collaboration purposes are now in place [17]. These concepts were taken into account in our study.

EXPERIMENTAL SETUP

The flow diagram shown in Figure 2 demonstrates the data-exchange process from CAD-to-CAM and CAD-to-CMM, using commercially available solutions. Rockwell Collins performed as the OEM. Rockwell Collins designed the test parts using Siemens NX™ CAD software.

Geater Machining and Manufacturing performed as the supplier. Geater used CNC Software's Mastercam® for numerical control programming for the manufacture (milling and turning) of the test parts. Geater used Mitutoyo MiCAT™ Planner automatic measurement program generation software to enable inspection of the test parts.

The data-exchange process required the use of CoreTechnologie 3D_Evolution© to convert data from the native NX™ CAD model into the standards-based STEP AP242 format. ITI PDElib® data exchange library was used to complete the import from STEP AP242 into Mastercam®. ITI eACIS utility library was used to complete the import from STEP AP242 into the ACIS® kernel used by MiCAT™ Planner.

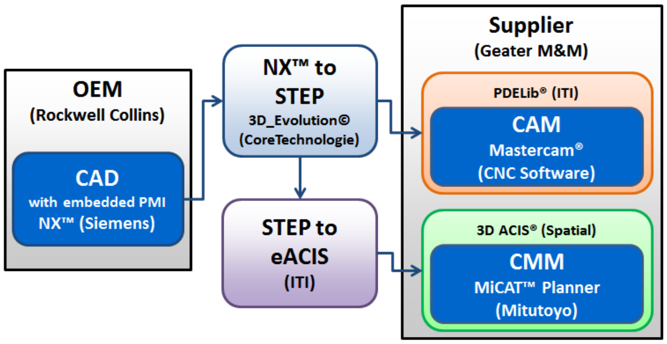
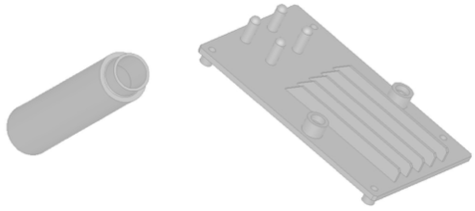


Figure 2: Data exchange process flow diagram

OEM and supplier components (see Figure 2) in the information-exchange process were analyzed to understand their constituent steps. The project team utilized two test cases – both a turned and a milled part. Figure 3 shows the test case models used in this project. Figure 3(a) is the turned test case and Figure 3(b) is the milled test case.

The OEM process steps – 3D-CAD-model creation and 2D-PDF-drawing creation – represent the activities most likely affected by the inclusion of embedded PMI in the CAD model necessary for downstream manufacturing and inspection. In addition to these activities, CAD tool issue resolution, designer education, as well as CAD model resolution to address CMM issues were also required. The OEM metrics captured for this research focus primarily on these CAD-model creation process steps, but also provide some insight into CAD-model validation and verification processes.

The CAM-process steps represent the activity involved in CAM-model creation. The project focused on those data elements most useful to the supplier for CAM-related process.



(a) Rolled Standoff (-903,-905,-907)

(b) Heat Sink (-904,-906,-908)

Figure 3. Test case models used in the project workflow

These elements demonstrate the difference between the current-state and the future-state process steps. They must provide enough detail to demonstrate the process areas significantly affected when ingesting models with embedded PMI for CAM programming. Finally, the elements need to align with the supplier process steps such that they can be easily recorded. The supplier completed the CAM-model-creation-process steps using the three technical data exchange scenarios and reported any observed data problems.

The project reviewed the manufacturing process steps identified in the NIST Testing the Digital Thread project [9]. The research compared these process steps to the manufacturing checklist steps used by the supplier. In the comparison, four general process step segments were identified.

Table 1: Process steps for manufacturing and inspection

Step	Manufacturing Process Steps	Inspection Project Steps
1	CAM Process Preparation	CMM Process Preparation
2	CAM Setup	CMM Setup
3	CAM Programming	CMM Programming
4	CAM Verification	CMM Verification
5		CMM Data Analysis

The CMM-process steps were identified in a similar way to the CAM process. Inspection steps previously defined in the NIST Testing the Digital Thread project [9] were compared to the steps in the supplier check-list for inspection. In the comparison, five general process step segments were identified. The final process steps are shown in Table 1.

As stated earlier, there are substantial benefits in switching from traditional 2D-drawing-based methods to 3D-model-based methods for transferring design information to manufacturing and inspection. However, product definitions are only useful to suppliers if the product-data quality is high. Verification of product-data quality in 2D drawings is done typically by visually inspecting the drawing for compliance with standards and best practices.

A standards-based workflow for design to manufacturing and inspection involves exchange of CAD-to-AP242-to-CAM-and-CMM models. Validation and verification of this translation process is critical, especially for regulated industries. An important part of quality assurance is traceability back to the design definition. To assure compliance at any point in the manufacturing or inspection process, it is essential to have validation and verification of the models throughout the data-exchange process.

When moving to a model-based paradigm, the verification process is more complex since the goal is for the model geometry and PMI to be consumed directly by downstream software systems. Verification in this context requires each and every PMI element be analyzed for syntactical and semantic accuracy, including proper association of the PMI to geometric references in the 3D geometry.

In addition to verifying that PMI content has been authored correctly, each time the data is transformed – from CAD to STEP and from STEP to CAM/CMM – the data must be validated to be sure no data corruption occurred during the transformation process. Since the information content in the 3D model is no longer in the form of a visually inspectable 2D drawing, software algorithms are required to perform the verification and validation processes on all but the simplest models.

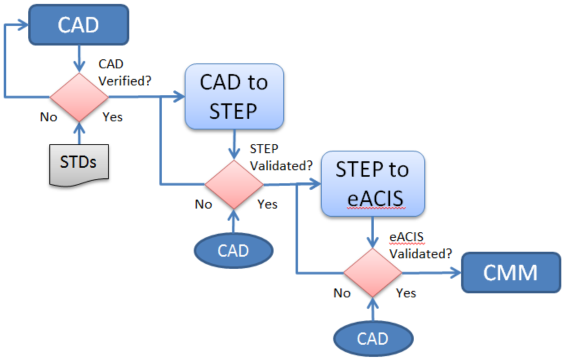


Figure 4: Verification and validation work-flow diagram

Real production models for two machined aerospace parts were used as the basis for testing the performance of the previously discussed processes and observing roadblocks that hampered process performance.

In the case of this experiment, the project team performed verification and validation following the work-flow outlined in Figure 4. The project team performed verification and validation using a combination of traditional visual inspection techniques and automated techniques. In general use on more complex models, automated techniques would have been required.

Table 2: CAD model creation metrics

CAD Metrics	***Rolled Standoff***			***Heat Sink***		
827-9999	**-903**	**-905**	**-907**	**-904**	**-906**	**-908**
2D PDF drawing	---	full dimension with 2D PMI annotation	key 2D PMI annotation only (PDD)	---	full dimension with 2D PMI annotation	key 2D PMI annotation only (PDD)
3D model	includes embedded PMI	not provided	with no embedded PMI	includes embedded PMI	not provided	with no embedded PMI
Number of PMI entities	23 (24*)	---	---	78 (90*)	---	---
CAD tool issue resolution and designer education	9.0 hours	0.5 hours	0.1 hours	4.9 hours	0.5 hours	0.1 hours
CAD model resolution to address downstream issues	2.3 hours + 4.5 hours to enhance process	---	---	3.0 hours + 1.3 hours to enhance process	original drawing missing dimension – rework required	---

* Original PMI entity count based on objects found in the NX Part navigator – eventually reduced count by issue resolution

RESULTS

Results from CAD Model Creation

Results and test case characteristics for the CAD model creation are shown in Table 2. For each test case, three data sets were generated. The future-state data sets (-903 and -904) included the 3D model (STEP AP242) with embedded PMI for the two test cases. The current state had two significant data sets to compare against the future state. The first current-state data set (-905 and -906) provided a full-annotated-2D drawing with dimensions and PMI. The part is represented fully and can be manufactured from the drawing. The second current-state data set (-907 and -908) contains the 3D-shape-geometry model (STEP AP203) and a 2D drawing with the PMI. The -907 and -908 data sets require both the model and the drawing together to manufacture the part.

Results from Mapping PMI between STEP and ACIS

The following PMI gaps were identified when mapping PMI between STEP AP242 and ACIS:

- Spherical dimension types (`RADIUS`, `DIAMETER`) are missing from ACIS
- Oriented and curved dimensions are missing from ACIS
- ACIS does not support angle selection (`SMALL`, `LARGE`, `EQUAL`) in an angular dimension
- Tolerance principal (`ENVELOPE`, `INDEPENDENCY`) is not supported by ACIS
- Dimension value with plus/minus bounds is not supported by ACIS
- Dimension value with qualifier (`MAXIMUM`, `MINIMUM`) is not supported by ACIS
- Limited support for dimension modifiers (`BASIC`, `REFERENCE`, `STATISTICAL`) by ACIS, many are missing (`CONTROLLED RADIUS`, `FREE STATE`, ANY CROSS SECTION, etc.)
- Movable datum target is not supported by ACIS
- Geometric tolerance type (`COAXIALITY`) is missing from ACIS
- Limited support for tolerance zone types (`DIAMETER`, `SPERICAL DIAMETER`, `PROJECTED`) by ACIS, some are missing (`NON-UNIFORM`, `RUNOUT`, `WITHIN A CIRCLE`, etc.)
- Limited to no support for tolerance modifiers (`FREE STATE`, `LMC`, `MMC`, `RFS`, `STATISTICAL`, `TANGENT PLANE`) by ACIS, many are missing (`ANY CROSS SECTION`, `COMMON ZONE`, etc.)
- Limited to no support for datum reference modifiers (`LMC`, `MMC`) by ACIS, many are missing (`FREE STATE`, `BASIC`, `TRANSLATION`, etc.)
- ACIS does not directly support POLYLINE presentation of PMI

Table 3: Validation of model transformations using embedded PMI entity count

PMI Elements (by format)	NX		STEP		ACIS		Mastercam		MiCAT	
Model (827-9999)	**-903**	**-904**	**-903**	**-904**	**-903**	**-904**	**-903**	**-904**	**-903**	**-904**
Dimension	8	54	8	54	8	54	8	54	8	54
Tolerance	6	13	6	13	6	13	6	13	6	13
Datum Feature	2	3	2	3	2	3	2	3	2	3
Notes (not semantic data)	7	8	7	8	0	0	7	8	0	0
Total	23	78	23	78	16	70	23	78	13	68

Results from Embedded PMI Data Exchange

Development and demonstration of a process to exchange standards-based models with embedded PMI from design to downstream systems was successful within the scope of the limited test models used in this project. The validation results, as defined by PMI element counts, for the downstream models are provided in Table 3. The validation shows that all dimensions, tolerances, and datum features were properly transformed and exchanged.

As indicated in Table 3, general notes could not be mapped to ACIS and were not transferable to the MiCAT Planner. Although manual validation showed correct PMI counts (for PMI other than general notes), further detailed examination by automated validation of the downstream models using analysis software found anomalies in the transformed data.

Table 4 shows the results of automated validation of model transformations. In the -904 model, the automated validation tool showed that though all dimensions were transformed and, for the most part, semantically correct, a rule violation occurred when the dimension tolerance zone for one dimension was considered too large relative to its nominal value. The -903 model, like the -904 model, was flagged for an instance of this same rule violation. The -903 model was also flagged for failure to maintain the semantic definition of limit dimensions in four instances of that dimension type when transformed from STEP to ACIS.

Table 4: Validation of models using analysis software

Model File	DFS[2] Clean	DIM[3] Clean	FCF[4] Clean	Clean Percent
827-9999-903	2	3	6	69%
827-9999-904	3	53	13	99%

The counts shown in Table 4 refer to the number of entities that are clean (e.g., pass all syntax and semantic validity checks during analysis of STEP to ACIS transformations). The clean percent ignores note entity errors.

DISCUSSION AND CONCLUSION

The results of this testing provide evidence to support the hypothesis that STEP AP242 with embedded PMI can successfully exchange model-based data from design (CAD) to manufacturing (CAM) and inspection (CMM). The experimental findings of our study fall within the areas of tools, standards, and process, as detailed below.

Tools

This research provides evidence that there is benefit from the CMM-system ability to interpret embedded-PMI information versus using nominal-shape-geometry-model dimensions. It is anticipated that the same benefit could be gained by CAM software as well. While the basic ability to receive the embedded PMI was achieved, the CAM tools require further development to fully leverage the benefit of receiving that data.

In a number of instances, embedded PMI created by the designer does not align well to the needs of downstream-machine consumption. Since PMI-authoring capabilities of CAD systems evolved from origins where 2D visualization of PMI was the requirement, current CAD systems allow designers to create PMI content that is, at best, only partially useable for downstream consumption. Embedded-PMI rules could be implemented in CAD systems to better align model creation with the downstream-machine-interpretation expectations.

CAD-model structures are also not optimized for downstream consumption. The ability to capture groupings of design features to represent geometric sets that correspond to equivalent manufacturing features is needed for downstream use and no method exists currently to achieve this functionality.

Standards

The project team recommends that the STEP community (standards development and implementer forum) should address certain gaps. During the course of the project, it was observed that there is incomplete PMI coverage and documentation of recommended practices for the standards.

[2] DFS = Datum Feature Symbol
[3] DIM = Dimension
[4] FCF = Feature Control Frame

Two examples illustrate the need for more coverage. There is the industry practice to use an unless-otherwise-specified tolerance callout as a general note. Although a workaround was achieved, a recommended practice is needed for this often-used callout to properly account for the required geometry associations.

The other example is surface-finish PMI, which is also not yet implemented by the STEP community. A development activity to support this construct is necessary. This also necessitates a recommended-practice document and the introduction of a test case into future test rounds of the STEP CAx Implementer Forum [18]. Formal extension of the ACIS format is also necessary for complete transformation of PMI data content.

Alternatively, the new Quality Information Framework[19] (QIF) format appears to show potential as a better standard for supporting inspection. In this project, QIF was also mapped against STEP and ACIS. QIF appears to be more complete than ACIS for PMI transfer. QIF also shows promise for allowing metrology results to be shared back to design. As a result, QIF may become the standard of choice for metrology, but additional research is necessary once downstream tools begin supporting QIF more widely as an import mechanism.

Processes

It was clear that designer education is not aligned with requirements for downstream-PMI consumption, especially for machine-interpretable expectations. Industry needs recommended practices for proper association of PMI to geometry elements.

There would also be value in a post-process to repair PMI geometry associations so they are complete and consistent. CAD systems should be augmented to provide design rules for creation of embedded PMI with downstream-machine consumption in mind or, at a minimum, recommended-practice documents need to be developed to guide designers as they annotate 3D models with PMI data.

Verification tools are needed to ensure that recommended practices are followed prior to the release of models for downstream consumption. Also, automated validation tools are required to insure information content is not lost or misinterpreted during transformation to formats needed for downstream consumption.

The latest version of AS9102 [20], the aerospace standard for reporting First Article Inspection (FAI) results, suggests potential exists to improve FAI reporting, particularly through automation. There is also potential for developing a visual presentation that integrates metrology results with MBD. Lastly, there is potential to provide metrology-results feedback to upstream users for analysis and prediction to better consider design decisions and manufacturing technologies for future products.

Summary

In summary, motivation exists for industry to continue its drive for the MBE vision through model-based data interoperability for design to manufacturing and quality inspection. A number of conclusions have been drawn from the research presented here. An attempt has been made to organize them broadly into categories of tools, standards, and processes.

Fundamentally, the project successfully demonstrated standards-based CAD-to-CAM and CAD-to-CMM data interoperability when using STEP AP242 with embedded PMI. In doing so, there were many issues uncovered — some the project team was able to address within the scope of the current research activity and others require further effort to overcome.

Some significant gaps were identified as well. These gaps will need to be addressed through changes in the tools, standards, and processes used currently to share information from design to manufacturing and inspection across the supply chain.

While this project was based upon a small-sample-size demonstration, the authors believe the results are potentially scalable for increased model complexity and PMI-element counts. Additionally, the project team tested the most popular modelling kernels used by CAM and CMM tools. The results suggest that the CAD/CAM/CMM workflow is scalable to all tools that use the ACIS or Parasolid geometric-modeling kernels. However, it is recommended that additional testing of the process be completed over a broader sample size.

Future research should seek opportunities to increase the number and variety of participants in the testing activity. This would result in a broader range of example data to work from and provide the opportunity to better assess the impact of variation in both design and processes.

Acknowledgments

The Engineering Laboratory of the National Institute of Standards and Technology (NIST) supported research reported in this paper under the following cooperative agreements:

- 70NANB14H314, International TechneGroup Incorporated, "Investigating the Impact of Standards-Based Interoperability for Design to Manufacturing and Quality in the Supply Chain"
- 70NANB14H256, International TechneGroup Incorporated, "Validation for Downstream Computer Aided Manufacturing and Coordinate Metrology Processes"

The contents of this report do not necessarily reflect the views of NIST. NIST and the authors do not make any warranty, expressed or implied, nor assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in the reports.

This paper may identify certain commercial systems. Such identification does not imply recommendation or endorsement by NIST, nor does it imply that the products identified are necessarily the best available for the purpose.

REFERENCES

[1] Wu, D., Rosen, D. W., Wang, L., and Schaefer, D., 2015, "Cloud-based design and manufacturing: A new paradigm in digital manufacturing and design innovation," Computer-Aided Design, 59(0), pp. 1-14. doi:10.1016/j.cad.2014.07.006

[2] Xu, X., 2012, "From cloud computing to cloud manufacturing," Robotics and Computer-Integrated Manufacturing, 28(1), pp. 75-86. doi:10.1016/j.rcim.2011.07.002

[3] Wu, D., Greer, M. J., Rosen, D. W., and Schaefer, D., 2013, "Cloud manufacturing: Strategic vision and state-of-the-art," Journal of Manufacturing Systems, 32(4), pp. 564-579. doi:10.1016/j.jmsy.2013.04.008

[4] Energetics Inc., 2015, "Measurement Science Roadmap for Prognostics and Health Management for Smart Manufacturing System," National Institute of Standards and Technology, Gaithersburg MD.

[5] Helu, M., and Hedberg Jr, T., 2015, "Enabling Smart Manufacturing Research and Development using a Product Lifecycle Test Bed," Procedia Manufacturing, 1, pp. 86-97. doi:10.1016/j.promfg.2015.09.066

[6] Gao, R., Wang, L., Teti, R., Dornfeld, D., Kumara, S., Mori, M., and Helu, M., 2015, "Cloud-enabled prognosis for manufacturing," CIRP Annals - Manufacturing Technology, 64(2), pp. 749-772. doi:10.1016/j.cirp.2015.05.011

[7] Li, M., Gao, S., and Wang, C. C., 2006, "Real-Time Collaborative Design With Heterogeneous CAD Systems Based on Neutral Modeling Commands," Journal of Computing and Information Science in Engineering, 7(2), pp. 113-125. doi:10.1115/1.2720880

[8] International Standards Organization, 2014, "Industrial automation systems and integration -- Product data representation and exchange -- Part 242: Application protocol: Managed model-based 3D engineering," ISO/TC 184/SC 4.

[9] Hedberg Jr, T. D., Lubell, J., Fischer, L., Maggiano, L., and Barnard Feeney, A., 2016, "Testing the Digital Thread in Support of Model-Based Manufacturing and Inspection," Journal of Computing and Information Science in Engineering. doi:10.1115/1.4032697

[10] International Standards Organization, 2010, "Industrial automation systems and integration -- Product data representation and exchange -- Part 214: Application protocol: Core data for automotive mechanical design processes," ISO/TC 184/SC 4.

[11] International Standards Organization, 2011, "Industrial automation systems and integration -- Product data representation and exchange -- Part 203: Application protocol: Configuration controlled 3D design of mechanical parts and assemblies," ISO/TC 184/SC 4.

[12] Hartman, N., Fischer, K., and Rosche, P., 2012, "Successfully engaging small and medium enterprises," 3D Collaboration and Interoperability CongressEnglewood CO.

[13] NIST MEP, 2009, "Phase One Final Report: Assessment of Supplier Capabilities to Operate in a Model-Based Enterprise Environment," National Institute of Standards and Technology, Manufacturing Extension Partnership, Gaithersburg MD.

[14] Feeney, A. B., 2002, "The STEP Modular Architecture," Journal of Computing and Information Science in Engineering, 2(2), pp. 132-135. doi:10.1115/1.1511520

[15] Barnard Feeney, A., Frechette, S. P., and Srinivasan, V., 2015, "A Portrait of an ISO STEP Tolerancing Standard as an Enabler of Smart Manufacturing Systems," Journal of Computing and Information Science in Engineering, 15(2), pp. 021001-021001. doi:10.1115/1.4029050

[16] International Standards Organization, 2006, "SASIG Product data quality guidelines for the global automotive industry," ISO/TC 184/SC 4.

[17] US Department of Defense, 2013, "Standard Practice: Technical Data Packages."

[18] PDES Inc., and ProSTEP iViP, 2014, "CAx Implementor Forum (CAx-IF)," https://cax-if.org/.

[19] Dimensional Metrology Standards Consortium, 2014, "Part 1: Overview and Fundamental Principles in Quality Information Framework (QIF) – An Integrated Model for Manufacturing Quality Information," Part 1: Overview and Fundamental Principles, American National Standards Institute.

[20] SAE International, 2014, "Aerospace First Article Inspection Requirement," SAE International,, Warrendale, PA.

Energy and Indoor Air Quality Benchmarking of the NIST Net-Zero Energy Residential Test Facility (NZERTF)

By

Tania Ullah, Dustin Poppendieck, William M. Healy, and A. Hunter Fanney, National Institute of Standards and Technology

and

Kevin Y. Teichman, U.S. Environmental Protection Agency

Poster presented at the

2016 American Council for an Energy Efficient Economy (ACEEE) Summer Study on Energy Efficiency in Buildings – Pacific Grove, CA

August 2016

SP-988

Ullah, Tania; Poppendieck, Dustin; Healy, William; Fanney, Arr; Teichman, Kevin.
"Energy and Indoor Air Quality Benchmarking of the NIST Net-Zero Energy Residential Test Facility (NZERTF)."
Paper presented at the 2016 ACEEE Summer Study on Energy Efficiency in Buildings, Pacific Grove, CA, Aug 21-Aug 26, 2016.

Energy and Indoor Air Quality Benchmarking of the NIST Net-Zero Energy Residential Test Facility (NZERTF)

Tania Ullah, Dustin Poppendieck, William M. Healy, and A. Hunter Fanney,
National Institute of Standards and Technology
Kevin Y. Teichman, U.S. Environmental Protection Agency

ABSTRACT

The National Institute of Standards and Technology (NIST) designed and built a residence that could generate, through the use of renewable energy systems, the amount of energy required by a virtual family of four over one year. The Net-Zero Energy Residential Test Facility (NZERTF) utilizes enhanced air sealing techniques, high levels of thermal insulation, and high-efficiency equipment to meet the comfort levels and functions of the virtual occupants while lowering energy consumption. Adequate ventilation and reduced indoor contaminant sources were also key design features to support occupant health and comfort.

The purpose of this paper is to assess how current and new approaches to benchmarking apply to high-performance homes. This study compares the annual energy use intensity (EUI) of the NZERTF (33.8 kWh/m^2 or 10.7 kBtu/ft^2) to the EUIs of existing single-family detached homes in the Mixed-Humid climate zone and the entire United States. The study presents the NZERTF's Home Energy Rating System (HERS) index (-6 with on-site power generation, 31 without), Home Energy Yardstick score (10), and the HUD Energy Benchmark Tool score (97). In contrast, indoor air quality (IAQ) benchmarking is challenging and not yet standardized. Concentrations of formaldehyde in the unoccupied NZERTF are typically above long-term non-carcinogenic relative exposure limits, but in the lowest 10th percentile compared to recent surveys of new, occupied homes. Concentrations of other volatile organic compounds (VOCs) in the NZERTF tend to be higher than these other homes, but below concentrations resulting in health concerns (except for acetaldehyde).

A truly high-performance residence must exceed both energy and IAQ benchmarks, as well as those related to thermal comfort, water consumption, and others. This work highlights the challenge in finding appropriate benchmarks to which a high-performance home should be compared.

Introduction

The Department of Energy (DOE) defines benchmarking as "the practice of comparing the measured performance of a device, process, facility, or organization to itself, its peers, or established norms, with the goal of informing and motivating performance improvement" (DOE 2016). One of the challenges in building energy benchmarking is identifying a representative building or set of buildings for comparison. An ideal benchmarking process entails comparing the rated building performance to that of reference buildings within the same climate zone, of the same size, housing type, number of occupants and occupant activities. For energy benchmarking of residential buildings, an extensive set of reference data can be obtained from the DOE Residential Energy Consumption Survey (RECS) (EIA 2009). The most recent version of RECS surveyed over 12,000 residential buildings of all types, and data were extrapolated to estimate

Ullah, Tania; Poppendieck, Dustin; Healy, William; Fanney, Arr; Teichman, Kevin.
"Energy and Indoor Air Quality Benchmarking of the NIST Net-Zero Energy Residential Test Facility (NZERTF)."
Paper presented at the 2016 ACEEE Summer Study on Energy Efficiency in Buildings, Pacific Grove, CA, Aug 21-Aug 26, 2016.

energy use and building characteristics of the 114 million residences in the nation's housing stock. The U.S. Department of Housing and Urban Development (HUD) carried out a similar, but less extensive survey, with public housing authorities to form the basis of their benchmarking tool (2007). Some energy benchmarking tools like the Residential Energy Services Network (RESNET) Home Energy Rating System (HERS) rely on simulations to generate a representative reference, which is the same building to the one that is rated, but modeled to minimum energy code requirements (ANSI/RESNET 2014).

Indoor environmental benchmarking efforts are less mature than those for energy, but are also very important. Minimizing occupant exposures to airborne contaminants should define IAQ benchmarking, regardless of whether it is achieved via increased ventilation (at an energy cost), filters (energy and financial cost), and/or reduced source emissions (potential financial cost). There are many challenges associated with benchmarking IAQ, however. These include identifying the most important pollutants to consider and selecting the concentration reference values to use for comparison. For example, benchmark comparisons can be made to health impact data or to concentrations in other existing homes. Further, if health impacts are used for comparisons, one must distinguish between benchmarks that refer to immediate or acute impacts and those that refer to long-term or chronic impacts. For many chemicals, there are no known health impact standards or recommendations, and comparisons can only be made to measured concentrations in existing housing stock.

In this work, energy and IAQ benchmarking was conducted at the Net-Zero Energy Residential Test Facility (NZERTF) located in Gaithersburg, MD, USA. This home was built as a research facility to assess various technologies and operational strategies for achieving net-zero energy operation through effective construction techniques, efficient equipment, and the use of photovoltaics. The house has a living area of 252 m^2 (2712 ft^2) and basement floor area of about 135 m^2 (1453 ft^2). Electrical energy and water use of two adults and two children is simulated throughout the year to provide a repeatable experiment to assess performance (Omar and Bushby 2013). The home was built with a highly insulated building envelope, an air and moisture control membrane. To comply with the minimum ventilation requirements in the ASHRAE Standard 62.2-2010 (ASHRAE 2010), a Heat Recovery Ventilator (HRV) was sized to deliver 137 $m^3\ h^{-1}$ of outdoor air but actually delivered 171 $m^3\ h^{-1}$ using the available fan speeds in the unit. Further details on the design of the home are provided by Pettit et al. (2014). This paper describes several approaches used to assess how this home's energy and indoor environmental quality performance compares to typical homes.

Energy Benchmarking of the NZERTF

NZERTF vs. Average Energy Use / Energy Use Intensity

One method to compare the NZERTF to reference housing stock is to use the Energy Use Intensity (EUI) metric or annual energy used per unit floor area. Similar metrics such as annual energy used per home, annual energy used per bed, or annual energy used per household member (Pérez-Lombard et al. 2009) exist but are less often used.

The NZERTF data acquisition system measured electrical energy every minute, both what was used by the virtual occupants of the home and the energy generated by the photovoltaic system. Details on the monitoring methodology can be found in Davis et al. (2014). The NZERTF consists of 252 m^2 (2712 ft^2) of living area (first and second floors) and 135 m^2 (1453 ft^2) of basement space, amounting to a total conditioned floor area of 387 m^2 (4165 ft^2). To remain consistent with the RECS survey, which monitors characteristics and energy consumption of a nationally representative sampling of homes, we did not include the detached garage or the attic in this analysis. The RECS survey only includes the garage if it is attached and conditioned and the attic if it is conditioned or finished, as well as the basement and other living areas of the home. During the first year of the home's operation, the NZERTF consumed a total of 13,039 kWh (44.5 MMBtu) of energy; thus, the EUI of the home is 33.8 kWh/m^2 (10.7 kBtu/ft^2).

The first five rows of Table 1 present average energy use per home and average EUIs, by housing characteristic, from the 2009 RECS database. The next three rows of Table 1 show data from the combined housing stock sharing two or more housing characteristics with the NZERTF. The NZERTF consumes approximately 49.6 % of the total energy of the average home in the U.S. (26,300 kWh/yr or 89.6 MMBtu/year) and has 23.5 % of its energy use intensity (144 kWh/m^2 or 45.5 kBtu/ft^2). The NZERTF performs similarly when compared to single-family detached homes and to all home types within the Mixed-Humid climate zone (the location of the NZERTF), with the NZERTF having 25.1 % and 23.5 % of their average EUIs, respectively.

Table 1. RECS 2009 Energy Performance Indicator (EPI) for Various Categories

Housing Characteristic	Avg. Energy Used per Yr		Avg. EUI	
	[kWh]	[*MMBtu*]	[kWh/m^2]	[*kBtu/ft^2*]
Average U.S. home	26,259	*89.6*	143.5	*45.5*
Single-Family Detached	30,978	*105.7*	134.4	*42.6*
Mixed-Humid (M-H) Climate Zone	26,816	*91.5*	140.1	*44.4*
Home built between 2000 and 2009	26,816	*91.5*	117.0	*37.1*
Total floor area ≥ 370 m^2 (4000 ft^2)	46,159	*157.5*	93.1	*29.5*
Single-Family Detached in M-H zone	31,359	*107.0*	129.0	*40.9*
Home built between 2000 and 2009, floor area ≥ 370 m^2 (4000 ft^2)	48,005	*163.8*	91.5	*29.0*
Single-Family Detached in M-H zone, built between 2000 to 2009, and floor area ≥ 370 m^2 (4000 ft^2)	45,719	*156.0*	89.9	*28.5*
NZERTF	**13,039**	***44.5***	**33.8**	***10.7***

One factor contributing to the low energy use intensity of the NZERTF is its size. In fact, home age and size are linked. Both the U.S. Census (Sarkar 2011) and the U.S. Energy Information Administration (EIA) (2015) have established the steady rise of detached single-family home floor area from 1980 to 2009; the average U.S. home grew 18.9 % in size in that period. The NZERTF is closer in energy performance to homes built in the last decade (EUI = 117.0 kWh/m^2 or 37.1 kBtu/ft^2) and even closer to other homes that have a total floor area of 370 m^2 (4000 ft^2) or more (EUI = 93.1 kWh/m^2 or 29.5 kBtu/ft^2). Furthermore, the combined factors of a home being built between 2000 and 2009 and having floor area greater than 370 m^2 (4000 ft^2) have a larger relation to the NZERTF EUI than homes that are detached single-family homes and are in the Mixed-Humid climate zone. The EUI of the former set of homes is 89.9 kWh/m^2 (28.5 kBtu/ft^2), and the EUI of the latter set is 129.0 kWh/m^2 (40.9 kBtu/ft^2). Comparing the NZERTF to houses of similar construction requires examining a subset of the RECS database that includes new, single-family detached housing located in Mixed-Humid climate zone with floor areas of 370 m^2 (4000 ft^2) or more. This group consumed on average of 89.9 kWh/m^2 (28.5 kBtu/ft^2) in 2009, compared to 33.8 kWh/m^2 (10.7 kBtu/ft^2) for the NZERTF (37.5 %).

HERS Index

In 1995, the National Association of State Energy Officials and Energy Rated Homes of America founded RESNET to develop a national standard for home energy performance ratings (RESNET 2016b). The RESNET process entails a visit from a certified home energy rating professional, during which the rater inspects characteristics such as insulation levels, window type, wall-to-window ratio, heating/cooling system efficiency, water heating system efficiency, solar orientation, and any renewable technologies (RESNET 2016b). The rater also collects airtightness data from blower door and duct leakage tests. HERS software calculates a score comparing a home's simulated energy use to that of the RESNET reference home. The reference home is simulated mostly to meet the 2006 International Energy Conservation Code and has shared characteristics to the rated home, such as gross floor area, foundation type, and fuel type (ANSI/RESNET 2014). A HERS Index Score of 100 means the rated home's predicted energy use is equivalent to that of the reference home. The lower the score, the more energy efficient the home. A HERS index of 80, for example, means that the rated home uses 20 % less energy compared to the reference home. Zero and negative scores of HERS are possible, since the calculation factors in on-site power production that offsets the electrical energy consumed in the home.

Including the solar thermal and photovoltaic systems on the home, the NZERTF has a HERS rating of -6; thus, the NZERTF *produces* 6 % more of the equivalent electrical energy that the RESNET reference home *consumes* overall. A recent report by RESNET (2016a) highlighted that the national average HERS index for net-zero homes was -7 (see Table 2).

Table 2. HERS index scores of non-net-zero energy and net-zero energy homes

Home type	HERS Index
Average U.S. net-zero home (n=185)	-7
Average Maryland net-zero home (n=2)	-2
NZERTF (as built)	**-6**
Average U.S. home (n=190,180)	62
Average Maryland home (n=5,903)	57
NZERTF (without on-site power production from PV)	**31**

Similar to the way energy benchmarking the NZERTF using RECS EUI data solely considered energy consumed, the HERS index can also be used to benchmark the NZERTF without the PV system. The HERS index in this case is 31; that is, the NZERTF without power generation on site is 69 % more energy efficient than the reference home. RESNET reports that the average HERS-rated home in the United States in 2015 received a score of 62 (2016c). Maryland homes rated by RESNET scored slightly better (average of 57) than the average rated U.S. home, possibly due to the fact that the state adopted the 2012 IECC and 2015 IECC building codes when they became available.

Benchmarking Tools for the Homeowner

While annual energy use/EUI and HERS index benchmarking provide useful comparisons of a rated home to the national building stock and a well-defined reference home, respectively, these benchmarking methods require expertise most homeowners do not have. They require careful tabulation of floor area from floor plans, detailed information about the walls, windows, appliances, and heating and cooling systems in the home, as well as results from air leakage tests. There are several simpler benchmarking tools available to the homeowner that can be used by inputting only a few housing characteristics, utility data, and location information.

The Home Energy Yardstick. The U.S. Environmental Protection Agency (EPA) Energy Star program has developed the Home Energy Yardstick rating system to provide homeowners with a performance-based energy comparison to similar homes (2016a). The tool uses 12 months of utility data with a statistical algorithm to control for the effects of location, home size, and number of occupants (all are inputs). The Yardstick algorithm compares the home to data obtained from the RECS. The Yardstick outputs a score from 1 to 10, where a “1” rated home uses more energy over 12 months than all comparable homes and a “10” performs at the top of the group. Using electrical energy consumption between July 2013 and June 2014, the NZERTF received a Yardstick score of 10.

HUD Utility Benchmarking Tool. The U.S. Department of Housing and Urban Development (HUD) has a spreadsheet tool to compare energy and energy costs of all types of residential buildings (single- and multi-family homes, attached and detached homes, etc.) to similar homes under public housing authorities (PHAs) (2007). Like the Home Energy Yardstick, the individual seeking a rating inputs zip code, annual energy used from all fuel types, and conditioned space floor area. A regression model algorithm generates the benchmarking score based on data voluntarily submitted for over 9,100 buildings by almost 350 PHAs nationwide. The tool outputs a score from 1 to 100, where a “50” is the HUD median home; the higher the score, the better. The HUD utility benchmarking tool gives the NZERTF a score of 97 compared to similar homes, with the HUD equivalent home (score = 50) having an EUI of 76.7 kWh/m^2 (24.3 kBtu/ft^2).

Indoor Air Quality Benchmarking of the NZERTF

The NZERTF was sampled monthly over 15 months to determine chemical concentrations of over 30 different chemicals (Poppendieck et al. 2015).[1] The chemicals measured in this study are not a comprehensive list of contaminants of concern. For example, fine particulate matter was not analyzed. Two sets of benchmarks were chosen to compare the NZERTF IAQ data: 1) U.S. governmental (federal and state) health guidelines, and 2) concentrations measurements from newly constructed homes.

Health Benchmarks

There are a wide range of health impacts that could be chosen as a health benchmark. Since the NZERTF is simulating a typical residence that would be occupied at least 15 hours a day, the most appropriate and conservative health benchmark would be a chronic rather than

[1] Note that indoor concentrations are shown in this document, while indoor minus outdoor concentrations are listed in Poppendieck et al. (2015).

acute benchmark. Seven of the 36 chemicals analyzed in the NZERTF have either a California Office of Environmental Health Hazard Assessment (OEHHA) chronic relative exposure level (CREL), an EPA inhalation reference concentration (RfC), or an EPA action level as shown in Table 3. Both CREL and RfC values define a concentration that is deemed to have no deleterious or cancerous impacts after a lifetime of exposure, e.g. eye, nose, or throat irritation.

Five of the analyzed chemicals have been classified as a known, probable, or possible human carcinogen according to the International Agency for Research on Cancer (IARC, references in Table 3). The EPA typically does not identify an acceptable exposure level to a carcinogen; rather, it defines unit risk factors to estimate cancer risk from chronic exposure to the chemical. Three of the studied chemicals have EPA inhalation unit risk factors (formaldehyde, acetaldehyde, and benzene). A user can choose an acceptable risk level and use the unit risk factor to determine the chemical concentration that correlates to that risk. A risk level of 1 cancer in 1,000,000 people is a typical risk level chosen for general public environmental exposure (e.g. Superfund sites), and a risk level of 1 cancer in 10,000 is a typical level chosen for individual workplace exposures. For the purpose of comparisons to the NZERTF concentration data these two risk levels were evaluated: 1 in 10,000 (10^{-4}) and 1 in 1,000,000 (10^{-6}).

The three chemicals with EPA unit risk factors (formaldehyde, acetaldehyde, and benzene) are highlighted below. For three of the other four chemicals listed in Table 3, the NZERTF concentrations were at least an order of magnitude below the CREL values.

Acetaldehyde. Acetaldehyde can be found in the indoor environment as the result of emissions from polyurethane foams and from secondary reactions of ozone and alkenes such as ethane. Acetaldehyde is considered a probable human carcinogen by IARC (2009). In monthly testing between May 2013 and July 2014, the NZERTF geometric mean concentration was 17.0 $\mu g/m^3$, with a maximum of 35.3 $\mu g/m^3$. A total of 13 of the 15 NZERTF samples exceeded the EPA RfC benchmark (9 $\mu g/m^3$), and all of the samples exceeded the carcinogenic inhalation exposure level correlating to a risk level of 10^{-6} (0.5 $\mu g/m^3$), indicating the NZERTF was frequently above these health benchmarks during normal operation. However, none of the samples exceeded the OEHHA CREL (140 $\mu g/m^3$) or the carcinogenic inhalation exposure level correlating to a risk level of 10^{-4} (50 $\mu g/m^3$). For reference, the outside acetaldehyde geometric mean concentration during the sampling events was 1.0 $\mu g/m^3$.

Benzene. Benzene can be released into the indoor environment from adhesives, sealants and attached garages with gasoline based engines. Benzene is classified as a human carcinogen (IARC 2012). The concentration of benzene in the NZERTF was typically below the method detection limit (MDL), always less than 1.1 $\mu g/m^3$, and never greater than 0.1 $\mu g/m^3$ above the outside concentration. For all samples, the benzene concentration was below the CREL value. The samples that exceeded the carcinogenic benchmark concentration correlating to a 10^{-6} risk level (0.45 $\mu g/m^3$) were typically attributable to elevated outdoor benzene levels.

Table 3. Summary of monthly chemical concentration measurements in NZERTF. (Numbers after the ± symbols are geometric standard deviations. Last column is number of measurements that exceeded a health reference level.)

Chemical	IARC Designation (Reference)	Agency (Ref)	Type	Bench-mark Conc.[a]	Geometric Mean of NZERTF Conc.	Times Benchmark Exceeded
Acetaldehyde	Probable Human Carcinogen (IARC 2009)	EPA (1988)	Carcinogenic 10^{-6}	0.5 µg/m^3	17 ± 1.7 µg/m^3	15
		EPA (1988)	Carcinogenic 10^{-4}	50 µg/m^3		0
		EPA (2000a)	RfC	9 µg/m^3		13
		OEHHA (2016)	CREL	140 µg/m^3		0
Benzene	Human Carcinogen (IARC 2012)	EPA (2000b)	Carcinogenic 10^{-6}	0.45 µg/m^3	MDL[b]	0
		EPA (2000b)	Carcinogenic 10^{-4}	45 µg/m^3		0
		OEHHA (2016)	CREL	3 µg/m^3		0
Formaldehyde	Human Carcinogen (IARC 2006)	EPA (1989)	Carcinogenic 10^{-6}	0.08 µg/m^3	9.2 ± 1.7 µg/m^3	15
		EPA (1989)	Carcinogenic 10^{-4}	8 µg/m^3		6
		OEHHA (2016)	CREL	9 µg/m^3		9
Ethylene Glycol	Not Listed	OEHHA (2016)	CREL	400 µg/m^3	14.2 ± 2.3 µg/m^3	0
Radon	Human Carcinogen (IARC 1988)	EPA (2016b)	Action Level	4 pCi/L	1.1 pCi/L	1[c]
Styrene	Possible Human Carcinogen (IARC 2002)	OEHHA (2016)	CREL	900 µg/m^3	2.6 ± 2.2 µg/m^3	0
Toluene	Not Listed	OEHHA (2016)	CREL	300 µg/m^3	2.2 ± 3.9 µg/m^3	0

[a] Benchmarks for carcinogens (known, probable, and possible) are the result of using the unit risk factors to calculate concentration that corresponds to a risk.

[b] MDL=method detection limit

[c] A total of twelve Radon samples were taken in the year (basement, first floor and second floor each quarter).

Formaldehyde. Formaldehyde can be released into the indoor environment from building materials including resins, insulation, and composite wood products (particleboard, medium density fiberboard, laminate flooring). Formaldehyde is classified as a human carcinogen (IARC 2006). The NZERTF had a geometric mean of 9.2 µg/m^3 with a maximum of 13.8 µg/m^3. A total of 9 of the 15 samples exceeded the non-cancer OEHHA CREL (9 µg/m^3). The NZERTF was below the CREL formaldehyde concentration only during winter months. All samples exceeded the carcinogenic benchmark concentration correlating to a 10^{-6} risk level (0.08 µg/m^3), while six samples exceeded the carcinogenic benchmark concentration correlating to a 10^{-4} risk level (8 µg/m^3). For reference, the outside formaldehyde geometric mean concentration during the sampling events was 1.4 µg/m^3.

Comparison Benchmarks

Many chemicals found indoors have no relevant health-based standard for comparison. Maddalena et al. (2012) found that of 235 chemicals identified in 108 new California homes, only 31 % had relevant health-based guidelines and less than 10 % had CRELs. An alternative benchmarking approach is to compare chemical concentrations to measurements in other residential structures. Two known recent, relatively large data sources for U.S. homes published by Hult et al. (2015) and Offermann (2009) are employed in this comparison.

Hult et al. (2015) analyzed 13 homes for formaldehyde and acetaldehyde concentrations. The homes were built with low-emitting materials meeting Leadership in Energy and Environmental Design (LEED)-certified/Indoor airPLUS criteria (further referred to as the "Indoor airPLUS study"). The furnished, occupied homes were less than five years old prior to the sampling event. Offermann (2009) measured 22 VOC concentrations in 108 new, single-family, occupied, detached homes built using standard construction methods in California (further referred to as the "California New Homes Study" (CNHS)). These homes were not built with specifications for low-emitting building materials. The homes were constructed between 2002 and 2004 and occupied at least one year prior to sampling. The California study determined the geometric mean concentration, a cumulative frequency distribution for each of the measured concentrations, and concentration percentiles for each chemical.

There are some differences between the homes in the two studies and the NZERTF that need to be taken into consideration when comparing their chemical concentrations. The homes in both studies were fully furnished and occupied, while the NZERTF was not furnished other than with built-in cabinets and had no occupants. The air change rate for homes in the Indoor airPLUS study (mean 0.26 h^{-1}, measured while VOC concentrations were measured, standard deviation 0.24 h^{-1}) and the CNHS (median 0.26 h^{-1}, measured during VOC sampling, mean 0.48 h^{-1}, standard deviation 0.78 h^{-1}) were higher than that of the NZERTF (mean 0.15 h^{-1}, total of measured mechanical ventilation and modeled infiltration during normal operation). It should be noted that 0.15 h^{-1} was calculated using the volume of the basement, 1st and 2nd floors, and attic. Given that the basement and attic were not directly ventilated by the HRV, 0.15 h^{-1} is not a measure of the removal rate of contaminants from the 1st and 2nd floors, where the air samples were taken. Nonetheless, the basement and attic were included in the calculated air change rate of 0.15 h^{-1} since both passively receive air from the 1st and 2nd floors through transfer grilles. Both the basement and attic are also within the conditioned space. If the basement and attic were not included, then the air change rate would be approximately 0.22 h^{-1}, not accounting for infiltration. The CNHS and studies both utilized perfluorocarbon tracer tests, which represented the total outdoor air ventilation rate delivered to the indoors. Given the lower air change rate in the NZERTF compared to the average homes in both studies, one would expect the concentration in the NZERTF to be higher for equal emission rates.

Table 4 compares the ten chemicals that were measured in both the CNHS Offermann (2009) and the NZERTF (Poppendieck et al. 2015). Formaldehyde and acetaldehyde comparisons to both the Indoor airPLUS study and the CNHS are highlighted below. The results of the remaining eight chemicals are discussed more briefly.

Table 4. A comparison of geometric means of ten chemical concentrations (μg/m^3) analyzed in both the NZERTF and the CNHS. The percentile is the minimum percentile rank (10 %, 25 %, 50 %, 75 %, or 90 %) statistically-derived from the CNHS, that the NZERTF did not exceed.

Compound	Max NZERTF Conc.	NZERTF Geometric Mean Conc.	Indoor airPLUS Homes Geometric Mean (Hult et al. 2015)	CNHS Geometric Mean Conc. (Offermann 2009)	NZERTF Percentile in the CNHS Study (Lower is better)[a]
Acetaldehyde	35.3	17.0 ± 1.7	33 ± 1.5	19 ± 2.3	50 %
Formaldehyde	13.8	9.2 ± 1.4	42 ± 1.4	36 ± 1.9	10 %
Hexanal	190	44.7 ± 2.5	N/A	7.0 ± 2.7	>90 %
Toluene	255	2.2 ± 3.9	N/A	9.5 ± 2.5	10 %
Styrene	9.8	2.6 ± 2.2	N/A	0.9 ± 2.8	90 %
1,2,4-Trimethylbenzene	7.8	3.7 ± 1.6	N/A	1.0 ± 3.2	90 %
Phenol	3.8	1.8 ± 1.6	N/A	1.6 ± 2.0	75 %
Ethylene glycol	37.6	14.2 ± 2.3	N/A	3.2 ± 5.6	75 %
α-Pinene	29.3	15.9 ± 1.4	N/A	9.3 ± 3.3	75 %
d-Limonene	4.3	1.8 ± 1.8	N/A	7.6 ± 5.0	25 %

[a] Lower numbers are better. Numbers after the ± represent geometric standard deviations.

Formaldehyde. Despite exceeding some formaldehyde health benchmarks, the NZERTF formaldehyde concentrations were lower than the other houses considered. This may be a function of the NZERTF not being furnished or occupied, both of which can contribute to elevated formaldehyde concentrations. The NZERTF geometric mean formaldehyde concentration was lower than all Indoor airPLUS homes and was in the lowest 10 % of measured formaldehyde concentrations in the CNHS. Homes in the Indoor airPLUS study were sampled during summer weather, which previous research has shown to lead to higher indoor concentrations of some VOCs (Poppendieck et al. 2015). The NZERTF formaldehyde geometric mean concentration during elevated summer months (May to September) was 11.8 μg/m^3, which is 36 % of the geometric mean value of the Indoor airPLUS homes.

Acetaldehyde. Despite exceeding acetaldehyde health benchmarks, the NZERTF acetaldehyde concentrations were lower or similar to the other houses considered. Only three of the 13 Indoor airPLUS homes had lower acetaldehyde concentrations than the geometric mean NZERTF concentration. The NZERTF acetaldehyde geometric mean concentration was below the geometric mean of the CNHS (Offermann 2009). The NZERTF acetaldehyde geometric mean concentration during summer months was 25.7 μg/m^3, which is 77 % of the average value of the 13 Indoor airPLUS criteria homes (sampled during summer months).

Other Chemicals. Eight other building material emission related chemicals are also listed in Table 4. For six of the eight remaining chemicals listed, the geometric mean concentration of the NZERTF samples was higher than that of the CNHS. This is in contrast to formaldehyde, where the NZERTF geometric mean concentration was lower than 98 % of the homes in the California study. Hence, for formaldehyde concentrations, the NZERTF outperforms these other homes built within a decade of its construction. This finding is likely due to the explicit construction specifications that limited formaldehyde in the building materials used and the fact that the NZERTF was not occupied or furnished. For most of the remaining chemicals in Table 4, there were no building specifications targeting these chemicals, due in part to lack of available content and emission data for these chemicals. In addition, the NZERTF has a lower air change rate than the average of the other data sets. Hence, one would expect if the emission rates are the same, the concentrations should be higher in the NZERTF. Even if the NZERTF does not perform better than comparable buildings with regards to these eight chemicals, for the three chemicals with health benchmarks listed in Table 3 (styrene, toluene, ethylene glycol), the geometric mean NZERTF concentrations are at least an order of magnitude below the health-based CRELs.

If a home designer or occupant finds that either desired health benchmarks or comparison benchmarks have not been met, reducing pollutant sources and/or increased ventilation can reduce indoor chemical concentrations. However, increased ventilation comes at a cost of increased energy use and the possibility of exceeding energy benchmarks.

Summary and Conclusions

Between July 2013 and June 2014, the Net-Zero Energy Residential Test Facility (NZERTF) in Gaithersburg, MD achieved net-zero energy consumption through the use of an on-site photovoltaic system, enhanced building envelope design, and efficient heating and cooling systems, appliances, and lighting. The home exceeded its goal and produced 484 kWh (1.65 MMBtu) of electrical energy that was returned to the grid. This study seeks to put the performance of the NZERTF into context by benchmarking for energy and indoor air quality. To summarize:

- The annual site energy use of the NZERTF was 13,039 kWh (44.5 MMBtu), 49.6 % of the national average (Table 1).
- The annual energy use intensity of the NZERTF was 33.8 kWh/m^2 (10.7 kBtu/ft^2), 23.5 % of the national average (Table 1).
- The NZERTF has a HERS index of -6 with photovoltaic energy generation and 31 without. This number compares well with the average HERS rated net-zero home (HERS = -7) and exceeds the average Maryland home (HERS = 57) (Table 2).
- The NZERTF has a Home Energy Yardstick score of 10 and a HUD Energy Benchmark score of 97.
- NZERTF concentrations of formaldehyde are in the lowest 10th percentile compared to recent surveys of new, occupied homes. However, these concentrations sometimes exceeded health benchmarks (Table 3).
- NZERTF concentrations of other volatile organic compounds (VOCs) on average tend to be higher than other homes surveyed (Table 4) and, with the exception of acetaldehyde, are below recommended exposure levels (Table 3).

High-performance-building designers desire a quantitative assessment of how energy upgrades and efforts to improve indoor air quality perform, but also need to be able to evaluate tradeoffs between the two goals. The authors contend that, while increasing energy efficiency and maintaining IAQ are linked, it is important to have standalone benchmarking evaluations of each, and a truly high-performance building would have high benchmarks for both. It has been established that energy benchmarking is a necessary tool for validating the design of homes like the NZERTF. The limitations in the past have been access to representative datasets and energy simulations, but that concern is no longer the case. The challenge for the indoor environment, however, is that there is no existing single benchmark metric for IAQ that allows comparisons among homes and such a benchmark may not be possible. In addition, datasets to support any benchmarks are lacking. Ideally there would be data available that summarizes the distribution of concentrations of hundreds of chemicals of concern in over a large number of residences both before and after occupation and in multiple climate regions. In addition, there would be known health impacts for both acute and lifetime exposures to all measured pollutants. More data are still needed to allow a proper discussion of what is “acceptable IAQ” in terms of measured pollutant concentrations.

Finally, this study illustrates a case of energy and IAQ benchmarking. There are other benchmarking metrics that have not been addressed which are still important in describing high-performance buildings. Thorough benchmarking should also consider thermal comfort, water usage, water quality, waste production, lighting quality, and acoustic performance, to name a few. Determination of representative datasets for benchmarking these aspects of a high-performance home may prove to be just as challenging as it is for IAQ.

References

ANSI/RESNET. 2014. Standard for the Calculation and Labeling of the Energy Performance of Low-Rise Residential Buildings using the HERS Index.

ASHRAE. 2010. Standard 62.2-2010: Ventilation and Acceptable Indoor Air Quality in Low-Rise Residential Buildings. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

Davis, Mark W, William M Healy, M Boyd, WV Payne, H Skye, and T Ullah. 2014. "Monitoring Techniques for the Net-Zero Energy Residential Test Facility." *NIST, Technical Note*.

DOE. 2016. "Building Energy Use Benchmarking." U.S. Department of Energy. Accessed February 17. http://energy.gov/eere/slsc/building-energy-use-benchmarking.

EIA. 2009. Residential Energy Consumption Survey (RECS). edited by EIA.

EIA. 2015. "Drivers of US Household Energy Consumption, 1980-2009." *Washington, DC, US Department of Energy*.

EPA. 1988. "Integrated Risk Information System (IRIS) - Acetaldehyde." Accessed March 11. https://cfpub.epa.gov/ncea/iris/index.cfm?fuseaction=iris.showQuickView&substance_nmbr=290.

EPA. 1989. "Integrated Risk Information System (IRIS) - Formaldehyde." Accessed March 11. https://cfpub.epa.gov/ncea/iris2/chemicalLanding.cfm?substance_nmbr=419.

EPA. 2000a. "Air Toxics Web Site - Acetaldehyde." Accessed March 11. https://www3.epa.gov/airtoxics/hlthef/acetalde.html.

EPA. 2000b. "Integrated Risk Information System (IRIS) - Benzene." Accessed March 11. https://cfpub.epa.gov/ncea/iris2/chemicalLanding.cfm?substance_nmbr=276.

EPA. 2016a. "Energy Star® Home Energy Yardstick." Accessed March 11. https://www.energystar.gov/index.cfm?fuseaction=HOME_ENERGY_YARDSTICK.showGetStarted.

EPA. 2016b. "Health Risk of Radon." Accessed March 11. https://www.epa.gov/radon/health-risk-radon.

HUD. 2007. Utility Benchmarking Tool. edited by HUD.

Hult, E. L., H. Willem, P. N. Price, T. Hotchi, M. L. Russell, and B. C. Singer. 2015. "Formaldehyde and acetaldehyde exposure mitigation in US residences: in-home measurements of ventilation control and source control." *Indoor Air* 25 (5):523-35. doi: 10.1111/ina.12160.

IARC. 1988. Man-made Mineral Fibres and Radon: Volume 43. In *IARC Monographs on the Evaluation of Carcinogenic Risks to Humans*. Lyon, France: World Health Organization.

IARC. 2002. Volume 82 Some Traditional Herbal Medicines, Some Mycotoxins, Naphthalene and Styrene. In *IARC Monographs on the Evaluation of Carcinogenic Risks to Humans*. Lyon, France: World Health Organization.

IARC. 2006. Volume 88 Formaldehyde, 2-Butoxyethanol and 1-tert-Butoxypropan-2-ol. In *IARC Monographs on the Evaluation of Carcinogenic Risks to Humans*. Lyon, France: World Health Organization.

IARC. 2009. "IARC Strengthens its Findings on Several Carcinogenic Personal Habits and Household Exposures." Accessed March 11. http://www.iarc.fr/en/media-centre/pr/2009/pdfs/pr196_E.pdf.

IARC. 2012. Chemical Agents and Related Occupations: Volume 100F A Review of Human Carcinogens. In *IARC Monographs on the Evaluation of Carcinogenic Risks to Humans*. Lyon, France: World Health Organization.

Maddalena, Randy, Na Li, Alfred Hodgson, Francis Offermann, and Brett Singer. 2012. "Maximizing Information from Residential Measurements of Volatile Organic Compounds." Healthy Buildings 2012, Brisbane, Australia.

OEHHA. 2016. "OEHHA Acute, 8-hour and Chronic Reference Exposure Level (REL) Summary." Accessed March 30. http://oehha.ca.gov/air/general-info/oehha-acute-8-hour-and-chronic-reference-exposure-level-rel-summary.

Offermann, Francis J. 2009. Ventilation and Indoor Air Quality in New Homes. California Energy Commission Contract 500-02-023, California Air Resources Board Contract 04-310.

Omar, F. , and S. T. Bushby. 2013. Simulating Occupancy in the NIST Net-Zero Energy Residential Test Facility. In *NIST Technical Note*: National Institute of Standards and Technology.

Pérez-Lombard, Luis, José Ortiz, Rocío González, and Ismael R Maestre. 2009. "A review of benchmarking, rating and labelling concepts within the framework of building energy certification schemes." *Energy and Buildings* 41 (3):272-278.

Pettit, Betsy, Cathy Gates, A Hunter Fanney, and William M Healy. 2014. Design Challenges of the NIST Net Zero Energy Residential Test Facility. In *NIST Technical Note*: National Institute of Standards and Technology.

Poppendieck, Dustin G., Lisa C. Ng, Andrew K. Persily, and Alfred T. Hodgson. 2015. "Long term air quality monitoring in a net-zero energy residence designed with low emitting interior products." *Building and Environment* 94:33-42. doi: 10.1016/j.buildenv.2015.07.001.

RESNET. 2016a. "103% Increase in the Number of HERS Rated Net Zero Energy Homes from 2013 to 2015." Last Modified February 18 Accessed February 24. http://www.resnet.us/blog/103-increase-in-the-number-of-hers-rated-net-zero-energy-homes-from-2013-to-2015/.

RESNET. 2016b. "Home Energy Ratings: A Primer." Accessed March 1. http://www.resnet.us/professional/ratings/HP05.

RESNET. 2016c. "Over 190,000 Homes in the U.S. Were RESNET HERS Rated and Issued a HERS Index Score in 2015 (30% Increase Over 2014)." Last Modified January 21 Accessed February 24. http://www.resnet.us/blog/over-190000-homes-in-the-u-s-were-resnet-hers-rated-and-issued-a-hers-index-score-in-2015-30-increase-over-2014/.

Sarkar, Mousumi. 2011. How American homes vary by the year they were built. Washington, DC: U.S. Census Bureau.

The Performance of an Auxiliary Heat Pump Water Heater Installed in a Dual-Tank System in a Net-Zero Energy Residence

By

T. Ullah and W. M. Healy, PhD
Energy and Environment Division
Engineering Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8632 USA

Presented at the ASHRAE Winter Conference – Orlando, FL
January 2016

Ullah, Tania; Healy, William.
"The Performance of an Auxiliary Heat Pump Water Heater Installed in a Dual-Tank System in a Net-Zero Energy Residence."
Paper presented at the ASHRAE Winter Conference 2016, Orlando, FL, Jan 23-Jan 27, 2016.

The Performance of an Auxiliary Heat Pump Water Heater Installed in a Dual-Tank System in a Net-Zero Energy Residence

Tania Ullah
Member ASHRAE

William M. Healy, Ph.D.
Member ASHRAE

ABSTRACT

In the effort to achieve low-energy operation of residential buildings, advanced water heating technologies are vitally important. This paper explores the year-long performance of a 189 L (50 gal) heat pump water heater (HPWH) serving as an auxiliary unit to an active, indirect solar thermal water heater with a 303 L (80 gal) storage tank in a net-zero energy test home located in Gaithersburg, MD, USA. The systems were subjected to a representative water use schedule for a virtual family of four between July 2013 and June 2014. We investigate the effect of inlet water temperature on the overall system Coefficient of Performance (COP_{sys}) of the HPWH and the unit's space conditioning impact, as these factors can vary substantially depending on the extent to which hot water demand is met by the solar thermal water heater. Field testing showed that the installed HPWH used 1104 kWh in the year and had a COP_{sys} of 1.41, not reaching the manufacturer's reported Energy Factor (EF) of 2.33 over the course of the 12-month testing period. The difference was largely due to the fact that the hot water load delivered by the unit was much less than if it were the sole water heater. The study of a HPWH in this unique configuration is valuable considering regulatory trends away from electric resistance storage water heaters, such as current standards in the United States that require EFs greater than 1.9 for electric water heaters with storage volumes greater than 208 L (55 gal).

INTRODUCTION

Water heating is the second largest energy consumer in homes, amounting to 18 % of the total energy use in residences (DOE 2012). For a high performance home, particular attention needs to be paid to minimizing all loads such that renewable technologies can provide the energy required to operate space heating and cooling equipment, water heaters, appliances, lighting, and plug loads. The Net-Zero Energy Residential Test Facility (NZERTF), a detached single-family test home built in Gaithersburg, Maryland, used the most energy efficient commercially-available water heating technologies. The primary means of water heating is accomplished with a solar thermal water heater. During times when solar irradiance is low or when hot water demand is high, this system would normally engage electric resistance elements in its storage tank for auxiliary heating. However, in the case of the NZERTF, auxiliary heating is instead provided by a heat pump water heater (HPWH) located downstream of the solar storage tank, making this a dual-tank water heating system. A two-tank configuration with an electric resistance water heater is not unusual, but the purpose of this paper is to provide data on how a HPWH performs in this scenario.

Tania Ullah is a mechanical engineer in the Energy and Environment Division, National Institute of Standards and Technology, Gaithersburg, MD. **William Healy** is the group leader of the Heat Transfer and Alternative Energy Systems Group, National Institute of Standards and Technology, Gaithersburg, MD.

Ullah, Tania; Healy, William.
"The Performance of an Auxiliary Heat Pump Water Heater Installed in a Dual-Tank System in a Net-Zero Energy Residence."
Paper presented at the ASHRAE Winter Conference 2016, Orlando, FL, Jan 23-Jan 27, 2016.

HPWHs use a vapor compression cycle to draw heat from the ambient air to heat water. Their recent popularity is highlighted by a U.S. Department of Energy (DOE) report stating that shipments of Energy Star® qualified integrated HPWHs increased 630 % between 2006 and 2009 (DOE 2010b). The presence of HPWH technology will increase furthermore in upcoming years due to DOE efficiency standards that require electric storage water heaters above 208 L (55 gal) to have a minimum Energy Factor (EF) of at least 1.9, depending upon storage volume (DOE 2010a).

In this paper, data from a field-tested HPWH in a dual-tank solar water heating system are provided to show how the increased inlet temperature affects its overall performance, and estimates are provided for comparison to an electric resistance unit that could be installed for auxiliary water heating in its place.

NZERTF DOMESTIC WATER HEATING

The NZERTF uses an active, closed-loop solar thermal system as its primary method for water heating. The system utilizes two solar collectors (1.1 m (3.8 ft) by 2.0 m (6.6 ft)) aperture dimensions, facing true south at an 18.4° tilt) and a 303 L (80 gal) storage tank with its auxiliary heating element disabled. In its stead, a HPWH provides hot water in the event that the solar thermal water heating system cannot meet the demand. The unit consists of a 189 L (50 gal) storage tank with an integrated air source heat pump and two 3800 W electric elements.

The HPWH was operated in the "Hybrid" mode with a temperature set-point of 48.9 °C (120.0 °F). The control logic of the HPWH in Hybrid mode is as follows: When the differential between the set-point temperature and the reading of a temperature sensor located in the top portion of the tank is 16.7 °C (30.0 °F) or more, the heat pump will turn off and the 3800 W top element will be energized. Once the top temperature sensor reading reaches the set-point, the element turns off and the heat pump comes on to heat the remainder of the tank (i.e., until the reading of the sensor at the bottom portion of the tank also reaches the set-point). While the HPWH has a second 3800 W electric element, it is not energized in this mode.

Hybrid mode ensures that the heat pump provides a majority of the hot water load while electric resistance is enlisted only when the heat pump cannot provide enough hot water. In the Hybrid mode, under test conditions of 57.2 °C (135.0 °F) set-point temperature and 19.7 °C (67.5 °F) ambient temperature, the manufacturer-reported EF, Coefficient of Performance (COP), and standby loss are 2.33, 2.36, and 0.20 °C/h (0.36 °F/h), respectively.

WATER USE CONTROL AND MONITORING

The NZERTF was used to demonstrate that a home similar in size and amenities to those in the surrounding community could generate as much energy through onsite renewable sources as used by a typical family of four (Fanney et al. 2015). The family was in fact a virtual family whose water-use and electricity-use behaviors were automated according to a weekly schedule derived from the Building America Research Benchmark Definition (Hendron and Engebrecht 2008). Over the course of each day, 44 water draws were initiated at the sinks, showers, and baths in the house by a real-time event controller according to a water draw schedule described by Omar and Bushby (2013). The clothes washer was initiated for two cycles each on three days of the week, and the dishwasher was initiated for a single cycle five days a week. Approximately 2570 L (680 gal) of mixed hot and cold water were utilized in the house per week.

The water temperature at the inlet and outlet of the HPWH storage tank and the ambient temperature were measured with immersed Type-T thermocouples with a calibrated uncertainty (k=2) of ± 0.1 °C (± 0.2 °F). The water flow through the solar thermal storage tank and the heat pump water heater was measured by pulse-output paddle-type flow meters with a resolution of 0.013 gal/pulse (0.049 L/pulse) and a calibrated uncertainty (k=2) within ± 1.7 % of reading. HPWH power was measured at the circuit breaker using current transformers with an uncertainty (k=2) that did not exceed ± 2 % of reading, and electrical energy use was determined from a time integration of power. Solar irradiance was measured with a pyronometer in the plane of the thermal collector array. Temperature and flow data were collected by the house data acquisition system and thermal energy calculations were made at 3-s intervals during water draw events, while the electrical energy data and ambient conditions were recorded every minute.

RESULTS AND DISCUSSION

Heat Pump Water Heater Efficiency

Table 1 shows monthly HPWH performance data for the year of testing. As a result of solar insolation and, thus, the water heating contribution of the solar thermal system varying monthly, the average HPWH inlet water temperature, $T_{HPWH,in}$, during times of draws ranged from a minimum of 23.3 °C (74.0 °F) in December to a maximum of 46.1 °C (114.9 °F) in June. This inlet temperature impacted the amount of time the heat pump and the heating elements operated according to the control logic explained above. The heat pump monthly total runtime ranged from a minimum of 57 h in June to a maximum of 178 h in January. The heating elements were inactive for all of June and active most often in November (partly on account of a defect with the heat pump unit). Likewise, the total electrical energy used by the HPWH, E_{HPWH}, ranged from 45 kWh in July to 156 kWh in December. The result was that the thermal energy contributed by the HPWH, $Q_{del,HPWH}$, reached its low in the summer (35 kWh in June) and peaked in the winter (244 kWh in December), as the solar thermal water heater's capacity to meet the virtual family's hot water demand changed seasonally. Q_{load} is the total energy in hot water delivered to fixtures and water-utilizing appliances.

The overall system Coefficient of Performance, COP_{sys}, is an efficiency metric that is the ratio of thermal energy delivered by the HPWH, $Q_{del,HPWH}$, to the electrical energy used to produce it, E_{HPWH}, computed as follows:

$$COP_{sys} = \frac{m \cdot c_p \cdot (T_{HPWH,out} - T_{HPWH,in})}{E_{HPWH}} \quad (1)$$

where m is the mass of hot water delivered to the fixtures, c_p is its specific heat, $T_{HPWH,out}$ is the outlet water temperature of the HPWH, and $T_{HPWH,in}$ is the inlet water temperature. The COP_{sys} is akin to the EF, although the rated EF is measured under specific test conditions outlined below from which the present HPWH operation deviates. HPWHs generally have EFs above 2.0 since the work done by the heat pump extracts heat from the surrounding air for water heating and the manufacturer of the NZERTF unit reports an EF of 2.33. Monthly COP_{sys} indicate that this level of efficiency is never reached; the COP_{sys} did not surpass 1.68 (January).

According to the DOE test method for rating residential water heaters in place at the time of the manufacturer's rating (DOE 2010a), HPWHs were subjected to a 24-h simulated use test where 243 L (64.3 gal) of hot water was drawn, maintaining the inlet temperature at 14.4 °C (58.0 °F) and the set-point at 57.2 °C (135.0 °F), for a target temperature rise of 42.8 °C (77.0 °F). As shown in Table 1, the average temperature rise (difference between the inlet and outlet water temperatures) was as low as 4.6 °C (8.3 °F) and as high as 25.4 °C (51.2 °F). As the mass of water drawn on a daily basis also changed depending on the day of the week, the daily thermal output of the HPWH, $Q_{del,HPWH}$, ranged from -2.0 kWh to 12.7 kWh, rather than being fixed at $Q_{del,sim\ use}$ = 11.9 kWh as it is during the 24-hour simulated use test. Figure 1 shows the daily COP_{sys} between July 2013 and June 2014 as a function of $Q_{del,HPWH}$. It should be noted that these data do not account for any changes in stored energy within the tank from the start to the end of the day. The hollow diamond symbols serve to differentiate the days in which electric resistance was used from the days in which only the heat pump operated (solid diamonds). The manufacturer-reported EF at $Q_{del,sim\ use}$ is placed on the plot (solid circle) as a reference to the HPWH performance under rating conditions.

Table 1. Monthly Heat Pump Water Heater Performance, July 2013 – June 2014

Month	Solar Insolation [kWh/m²]	$T_{basement}$ [°C] ([°F])	RH [%]	$T_{HPWH,in}$ [°C] ([°F])	$T_{HPWH,out}$ [°C] ([°F])	HP Run Time [h]	Elmnt. Run Time [h]	Q_{load} [kWh]	$Q_{del,HPWH}$ [kWh]	E_{HPWH} [kWh]	COP_{sys}
Jul[a]	152	21.6 (70.8)	52.2	43.2 (109.8)	51.6 (124.9)	56	0	252	42	45	0.93
Aug[a,b]	123	21.7 (71.0)	51.4	35.7 (96.3)	51.8 (125.3)	86	2	218	108	71	1.52
Sep	158	22.1 (71.9)	51.9	41.8 (107.2)	51.5 (124.7)	69	1	238	68	57	1.20
Oct	114	21.2 (70.2)	51.6	37.6 (99.6)	51.6 (124.9)	105	1	269	119	82	1.44
Nov[c]	102	20.4 (68.8)	41.2	30.5 (86.9)	52.0 (125.6)	113	11	283	172	130	1.32
Dec[c]	73	20.1 (68.1)	38.0	23.3 (74.0)	51.8 (125.2)	160	10	326	244	156	1.56
Jan	101	19.8 (67.6)	31.4	23.7 (74.6)	51.3 (124.4)	178	4	343	240	143	1.68
Feb	98	19.5 (67.2)	30.7	25.6 (78.0)	51.3 (124.3)	153	4	330	208	125	1.66
Mar	117	19.5 (67.1)	30.6	28.8 (83.9)	51.3 (124.3)	149	4	341	187	121	1.55
Apr	153	19.6 (67.3)	40.0	38.9 (102.1)	49.9 (121.9)	92	1	300	84	73	1.16
May	161	20.8 (69.4)	51.6	44.2 (111.5)	50.9 (123.6)	69	0[d]	277	55	55	0.99
June	164	21.3 (70.3)	53.3	46.1 (114.9)	50.7 (123.2)	57	0	251	35	46	0.77
Year Total	**1518**					**1287**	**38**	**3428**	**1563**	**1104**	
Year Avg		**20.6** **(69.1)**	**43.6**	**34.9** **(94.9)**	**51.3** **(124.4)**						**1.41**

[a] Data loss on 7/1/2013 and 8/2/2013 – 8/6/2013; therefore, monthly values in table exclude these days.

[b] Between 8/24/2013 and 9/3/2013, the pumps of the solar thermal water heater heat exchanger were not operational due to failure of electrical connection to glycol circulating pump.

[c] Between 11/25/2013 and 12/5/2013, the heat pump of the heat pump water heater was not operational due to a control wire being disconnected.

[d] Resistance element run time in May was not "0" but a very small value rounded to 0.

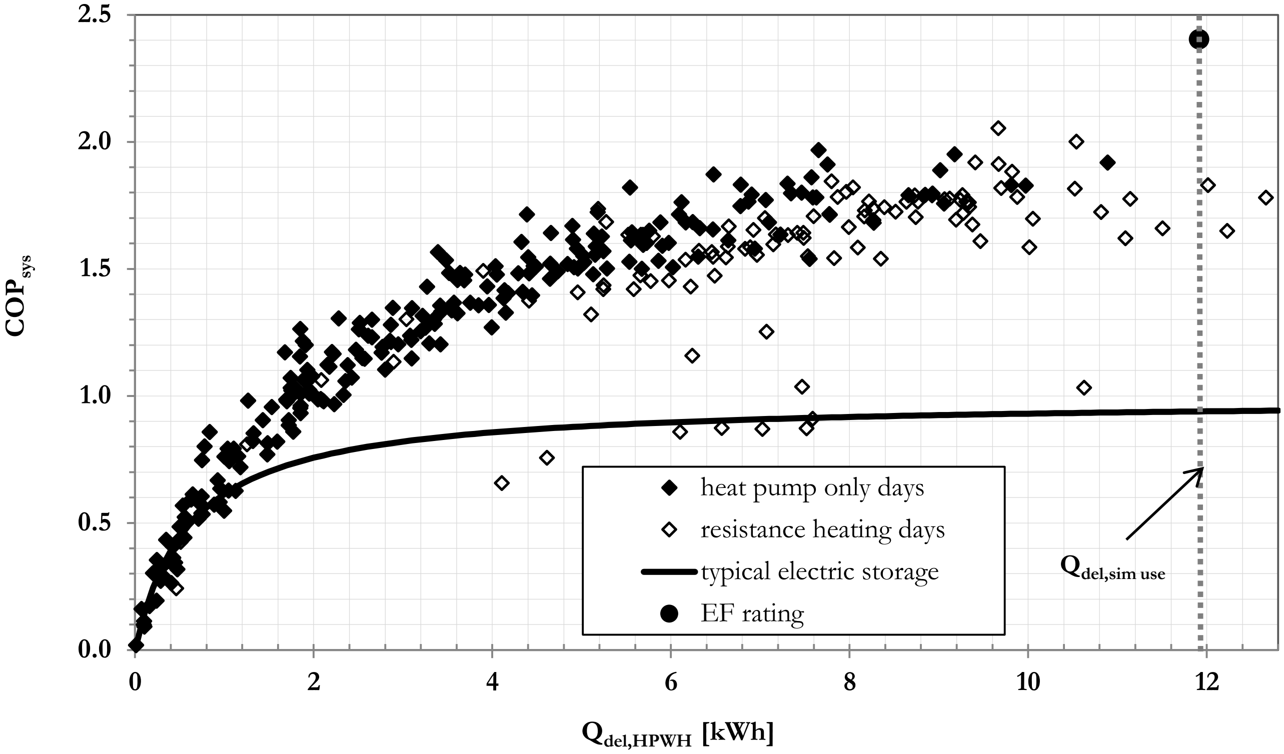


Figure 1 Daily averaged overall system Coefficient of Performance (COP$_{sys}$) of the heat pump water heater as a function of its thermal output, July 2013 – June 2014.

The overall COP$_{sys}$ of any storage-type water heater will decline as the thermal output of the water heater goes to zero, i.e., as the temperature entering the unit nears the set-point temperature. This condition happens because of two factors: (1) the numerator in Equation 1 goes to zero, and (2) the water heater heater must have a minimum amount of electrical energy input on a daily basis to make up for thermal standby losses. For HPWHs, an added effect is that the refrigerant-to-water heat exchange efficiency decreases as the temperature of the water entering the heat pump compressor increases. While the installed unit is capable of reaching its rated efficiency, it does not operate under the conditions that would allow it to do so for most days of the year.

In addition to the daily COP$_{sys}$ shown in Figure 1, the data are compared to a COP$_{sys}$ curve (solid black line) that has been calculated for a typical electric storage water heater using equations from the Water Heater Analysis Model (WHAM) (Lutz et al. 1998). This theoretical unit has a rated EF of 0.95 and recovery efficiency, η_{rec}, of 0.98, but it operates with a tank temperature set-point of 48.9 °C (120.0 °F) as is the case for the HPWH under test. At $Q_{del,sim\ use}$, the COP$_{sys}$ of the NZERTF HPWH is 2.5 times greater than the COP$_{sys}$ of an electric storage water heater determined using WHAM to adjust for the different stored water temperature. However, that factor diminishes as the HPWH delivers less thermal energy; at approximately $Q_{del,HPWH} \approx 1$ kWh and below, the COP$_{sys}$ data for the HPWH (diamond symbols) and the electric storage curve (black line) converge. In this range of water heater delivered energy, the HPWH no longer is more efficient than an electric storage water heater. For the period between July 2013 and June 2014, the HPWH delivered less than 1 kWh of thermal energy as hot water for 68 d (19 %) out of the 359 d examined.

Overall Energy Use

The expected benefit of an air-to-water heat pump is that energy usage for water heating can be cut by a factor of 2 or more as determined by rating tests. An electric storage water heater with an EF of 0.95 uses 4622 kWh of electrical energy per year when subject to conditions specified in the DOE test procedure in effect prior to July 2014, and a HPWH with an EF of 2.33 uses 1866 kWh under those same conditions. However, the field-testing discussed here of a HPWH serving as an auxiliary heater to another water heater under typical use conditions indicates that the heat pump water heater efficiency can vary significantly because of deviation from rating test conditions.

For the July 2013 to June 2014 period, the HPWH in the NZERTF used 1104 kWh. To compare to an electric resistance unit, it is estimated using the WHAM model that an electric resistance water heater would have consumed 1851 kWh to deliver the same amount of energy if it were installed in the NZERTF as an auxiliary unit to the solar thermal water heater. At an average residential retail electricity price of $0.12 per kWh (EIA 2015), the heat pump water heater would cost $133 to operate for the year while the electric resistance unit is estimated to cost $222. The HPWH exhibited an overall system Coefficient of Performance of 1.41 for the year, while the electric resistance unit would have had a COP_{sys} of 0.86.

The HPWH fell short of its rating for a number of reasons. First, the delivered energy was much lower than at the rated value. Second, the rated value likely does not include situations when the electric resistance element was activated, since the water draws conducted during the test method do not always activate the elements. Figure 1 shows that for a significant number of days in the year, resistance heating was needed at the NZERTF. Finally, the efficiency of the heat pump's vapor compression system is lower at the higher inlet water temperatures experienced at the NZERTF as compared to the simulated use test. While the rated EF of the HPWH was 145 % greater than the rated value of a resistance water heater, the measured COP_{sys} of the HPWH over the year of operation was only 64 % greater than the estimated COP_{sys} of the resistance water heater. Nevertheless, the use of the HPWH saved $89 over the year compared with an electric resistance unit.

Space Conditioning Impact

Air-to-water heat pump operation extracts heat from the zone in which the water heater is installed. While a detailed analysis of the impacts of the HPWH on space conditioning loads is beyond the scope of this paper, a few points on this topic are worth mentioning. Figure 2 shows how space conditioning is impacted by the temperature of the water entering the HPWH. As detailed in Sparn et. al (2013), $Q_{net,space}$, the net energy added to the space, is determined as follows:

$$Q_{net,space} = Q_{loss} - Q_{air} = E_{HPWH} - Q_{del,HPWH} \qquad (2)$$

where Q_{loss} is energy lost from the tank surface and Q_{air} is heat transferred from the air to the tank via the heat pump. A negative $Q_{net,space}$ means that more energy is being transferred to heat water than is lost to the zone. In Figure 2, the triangular symbols indicate days in which the whole house air-to-air heat pump was in heating mode, while the circular symbols represent days in which the air-to-air heat pump was in cooling mode. Furthermore, the hollow symbols differentiate days in which the electric elements were engaged from the days in which only the air-to-water heat pump alone supplied heat to the water (solid symbols).

The net space conditioning predicted by a linear regression of all data in Figure 2 indicates that, at the test condition of inlet temperature $T_{inlet,sim\ use}$ = 14.4 °C (58.0 °F), 4.34 kWh of heat will be removed from the space (negative $Q_{net,space}$). Thus, 4.34 kWh more energy would have to be supplied to the space by the HVAC system to maintain the basement ambient temperature. Inlet water temperature would only ever be that low when solar thermal water heater output is low in the heating season. There are only 3 d in which the inlet water temperature is at or below $T_{inlet,sim\ use}$ and the $Q_{net,space}$ at the minimum average daily inlet temperature during the testing period was -5.21 kWh.

Additionally, the data indicate that at a daily average inlet water temperature of approximately 43.3 °C (110.0 °F), a changeover occurs where the energy losses from the tank begin to outweigh the energy transfer by the heat pump of the water heater (a positive $Q_{net,space}$). While the HPWH receives incoming water from the solar thermal storage tank over a wide range of temperatures, 13.1 °C (55.5 °F) to 54.7 °C (130.5 °F) between July 2013 and June 2014, respectively, the HPWH inlet temperature exceeded 43.3 °C (110.0 °F) 95 d (26 %) out of 359 d. Those days occurred mostly in the cooling season and, thus, more energy would have to be extracted from the space by the HVAC system as a result of HPWH operation. $Q_{net,space}$ = 1.68 kWh was added to the space by the HPWH on the day of highest inlet water temperature in the testing period.

It should be noted that an electric resistance water heater would only add heat to the space and would not have the ability to remove it. In other words, the $Q_{net,space}$ associated with an electric resistance water heater would always be positive, whereas sometimes the $Q_{net,space}$ associated with a HPWH is positive (generally cooling season) and sometimes it is negative (generally heating season). While the net space conditioning impacts of the HPWH on the zone has been quanitifed above, the degree to which this impacts the heating and cooling loads of the whole house air-to-air heat pump will be studied in the future.

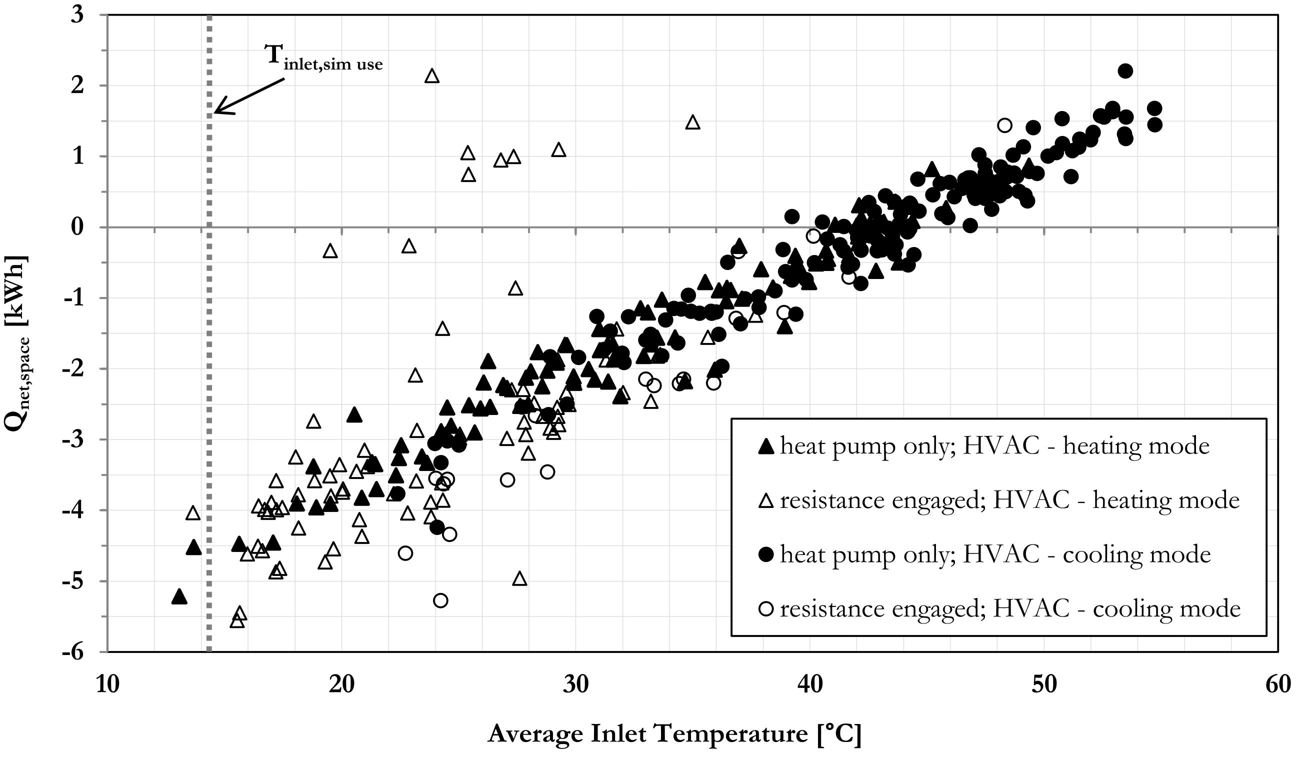


Figure 2 Net thermal energy transferred to basement zone as a function of inlet water temperature, July 2013 – June 2014.

CONCLUSIONS

A dual-tank water heating system that employs a heat pump water heater (HPWH) for auxiliary heating to a solar thermal system used less energy than would be expected with an electric resistance water heater, but exhibited overall system Coefficients of Performance ($\mathrm{COP}_{\mathrm{sys}}$) below what ratings data indicate during times when the solar thermal system was providing the majority of hot water required for occupant use. While the rated EF of the unit is 2.33, the average $\mathrm{COP}_{\mathrm{sys}}$ of the HPWH over a year-long period was 1.41. This decrease is partially due to the fact that the amount of thermal energy delivered by the water heater is much lower than is required during the rating test given a lower temperature rise from inlet to outlet and a lower volume of delivered hot water. The average inlet water temperature of the HPWH was 34.9 °C (94.8 °F) compared to 14.4 °C (58.0 °F) as prescribed in the test procedure, and the average delivered water temperature was 51.3 °C (124.4 °F) compared to the value of 57.2 °C (135 °F) prescribed in the test procedure. An added factor is that the performance of the heat pump unit drops with higher inlet water temperature. With this reduced thermal energy demand, it was estimated that an electric resistance water heater would have operated at an efficiency of 0.86. The average $\mathrm{COP}_{\mathrm{sys}}$ of the HPWH of 1.41 makes it only 64 % more efficient than a standard electric storage water heater rather than 145 % more efficient as suggested by the ratings. Nevertheless, the annual energy consumption of the HPWH was estimated to be 747 kWh less than what would have been expected if an equivalently sized electric resistance water heater having an EF of 0.95 were installed as an auxiliary water heater to the solar thermal system as opposed to the HPWH. The net energy transferred to the space, $Q_{\mathrm{net,space}}$, was found to follow a linear trend with the inlet water temperature. The data indicate that the maximum thermal energy removed from the basement zone during a single day due to HPWH operation is 5.21 kWh, and that day occurred in the heating season. Additionally, the maximum thermal energy added to the basement zone during a single day due to HPWH operation is 1.68 kWh, which occurred in the cooling season. The extent to which $Q_{\mathrm{net,space}}$ has an impact on whole-house HVAC operation is to be determined in future research.

ACKNOWLEDGEMENTS

The authors acknowledge the contributions of Mark W. Davis, mechanical engineer formerly at the Engineering Laboratory at NIST, and Al Collins, software engineer at Acquired Data Solutions for assisting with data collection and management.

REFERENCES

DOE. 2010a. Energy Conservation Program: Energy Conservation Standards for Residential Water Heaters, Direct Heating Equipment, and Pool Heaters; Final Rule. *Federal Register,* Vol. 75, No. 73.

DOE. 2010b. Energy Star (R) Water Heater Market Profile. http://www.energystar.gov/ia/partners/prod_development/new_specs/downloads/water_heaters/Water_Heater_Market_Profile_2010.pdf.

DOE. 2012. 2011 Buildings Energy Data Book. http://buildingsdatabook.eren.doe.gov.

EIA. 2015. Electric Power Monthly with Data for April 2015. http://www.eia.gov/electricity/monthly/pdf/epm.pdf.

Fanney, A. H., Payne, V., Ullah, T., Ng, L., Boyd, M., Omar, F., Davis, M., Skye, H., Dougherty, B., Polidoro, B., Healy, W., Kneifel, J., and Pettit, B. 2015. Net-zero and beyond! Design and performance of NIST's net-zero energy residential test facility. *Energy and Buildings,* 101 (0): 95-109. doi: http://dx.doi.org/10.1016/j.enbuild.2015.05.002

Hendron, R., and Engebrecht, C. 2008. Building America Research Benchmark Definition, National Renewable Energy Laboratory. http://apps1.eere.energy.gov/buildings/publications/pdfs/building_america/44816.pdf.

Lutz, J., Whitehead, C. D., Lukov, A., Winiarski, D., and Rosenquist, G. 1998. WHAM: A Simplified Energy Consumption Equation for Water Heaters. In *Proceedings of the 1998 ACEEE Summer Study on Energy Efficiency in Buildings.* http://aceee.org/files/proceedings/1998/data/papers/0114.PDF.

Omar, F., and Bushby, S. T. 2013. Simulating Occupancy in the NIST Net-Zero Energy Residential Test Facility. NIST TN - 1817. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=914650.

Sparn, B., Earle, L., Christensen, D., Maguire, J., Wilson, E., and Hancock, C. 2013. Field Monitoring Protocol: Heat Pump Water Heaters. http://www.nrel.gov/docs/fy13osti/57698.pdf.

Limiting the Impact of Stealthy Attacks on Industrial Control Systems

David I. Urbina[1], Jairo Giraldo[1], Alvaro A. Cardenas[1], Nils Ole Tippenhauer[2], Junia Valente[1], Mustafa Faisal[1], Justin Ruths[1], Richard Candell[3], and Henrik Sandberg[4]

[1]University of Texas at Dallas, [2]Singapore University of Technology and Design, [3]National Institute of Standards and Technology, and [4]KTH Royal Institute of Technology

{david.urbina, jairo.giraldo, alvaro.cardenas, juniavalente, mustafa.faisal, jruths}@utdallas.edu, nils_tippenhauer@sutd.edu.sg, richard.candell@nist.gov, and hsan@kth.se

ABSTRACT

While attacks on information systems have for most practical purposes binary outcomes (information was manipulated/eavesdropped, or not), attacks manipulating the sensor or control signals of Industrial Control Systems (ICS) can be tuned by the attacker to cause a continuous spectrum in damages. Attackers that want to remain undetected can attempt to hide their manipulation of the system by following closely the expected behavior of the system, while injecting just enough false information at each time step to achieve their goals.

In this work, we study if physics-based attack detection can limit the impact of such stealthy attacks. We start with a comprehensive review of related work on attack detection schemes in the security and control systems community. We then show that many of these works use detection schemes that are not limiting the impact of stealthy attacks. We propose a new metric to measure the impact of stealthy attacks and how they relate to our selection on an upper bound on false alarms. We finally show that the impact of such attacks can be mitigated in several cases by the proper combination and configuration of detection schemes. We demonstrate the effectiveness of our algorithms through simulations and experiments using real ICS testbeds and real ICS systems.

Keywords

Industrial Control Systems; Intrusion Detection; Security Metrics; Stealthy Attacks; Physics-Based Detection; Cyber-Physical Systems

1. INTRODUCTION

One of the fundamentally unique and intrinsic properties of Industrial Control Systems (ICS)—when compared to general Information Technology (IT) systems— is that changes in the system's state must follow immutable laws of physics. For example, the physical properties of water systems (fluid dynamics) or the power grid (electromagnetics) can be used to create prediction models that we can then use to confirm that the control commands sent to the field were executed correctly and that the information coming from sensors is consistent with the expected behavior of the system: if we opened an intake valve, we would expect the water tank level to rise, otherwise we may have a problem with the control, actuator, or the sensor.

The idea of using physics-based models of the normal operation of control systems to detect attacks has been used in an increasing number of publications in security conferences in the last couple of years. Applications include water control systems [21], state estimation in the power grid [35, 36], boilers in power plants [67], chemical process control [10], electricity consumption data from smart meters [40], and a variety of industrial control systems [42].

The growing number of publications shows the importance of leveraging the physical properties of control systems for security; however, a missing element in this growing body of work is a unified adversary model and security metric to help us compare the effectiveness of previous proposals. In particular, the problem we consider is one where the attacker knows the attack-detection system is in place and bypasses it by launching attacks imitating our expected behavior of the system, but different enough that over long periods of time it can drive the system to an unsafe operating state. This attacker is quite powerful and can provide an upper bound on the worst performance of our attack-detection tools.

Contributions. (i) We propose a strong adversary model that will always be able to bypass attack-detection mechanisms and propose a new evaluation metric for attack-detection algorithms that quantifies the negative impact of these stealthy attacks and the inherent trade-off with false alarms. Our new metric helps us compare in a fair way previously proposed attack-detection mechanisms.

(ii) We compare previous attack-detection proposals across three different experimental settings: a) a testbed operating real-world systems, b) network data we collected from an operational large-scale Supervisory Control and Data Acquisition (SCADA) system that manages more than 100 Programmable Logic Controllers (PLCs), and c) simulations.

(iii) Using these three scenarios we find the following results: (a) while the vast majority of previous work uses stateless tests on residuals, stateful tests are better in limiting the impact of stealthy attackers (for the same levels of false alarms), (b) limiting the impact of a stealthy attacker can also depend on the specific control algorithm used and not only on the attack-detection algorithm, (c) linear state-space

Publication rights licensed to ACM. ACM acknowledges that this contribution was authored or co-authored by an employee, contractor or affiliate of the United States government. As such, the Government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for Government purposes only.

CCS'16, October 24 - 28, 2016, Vienna, Austria

© 2016 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 978-1-4503-4139-4/16/10…$15.00

DOI: http://dx.doi.org/10.1145/2976749.2978388

Urbina, David; Cardenas, Alvaro; Tippenhauer, Niles O.; Valente, Junia; Faisal, Mustafa; Ruths, Justin; Candell Jr., Richard; Sandberg, Heinrik. "Limiting The Impact of Stealthy Attacks on Industrial Control Systems."
Paper presented at the 23rd ACM Conference on Computer and Communications Security, Vienna, Austria, Oct 24-28, 2016.

models outperform output-only autoregressive models, (d) time and space correlated models outperform models that do not exploit these correlations, and (e) from the point of view of an attacker, launching undetected actuator attacks is more difficult than launching undetected false-data injection for sensor values.

The remainder of this paper is organized as follows: In § 2, we provide the scope of the paper, and provide the background to analyze previous proposals. We introduce our attacker model and the need for new metrics in § 3. We introduce a way to evaluate the impact of undetected attacks and attack-detection systems in § 4, and then we use this adversary model and metric to evaluate the performance of these systems in physical testbeds, real-world systems, and simulations in § 5.

2. BACKGROUND AND TAXONOMY

Scope of Our Study. We focus on using real-time measurements of the physical world to build indicators of attacks. In particular, we look at the physics of the process under control but our approach can be extended to the physics of devices as well [18]. Our work is motivated by false sensor measurements [35, 58] or false control signals like manipulating vehicle platoons [19], manipulating demand-response systems [58], and the sabotage Stuxnet created by manipulating the rotation frequency of centrifuges [17, 32]. The question we are trying to address is how to detect these false sensor or false control attacks in real-time.

2.1 Background

A general feedback control system has five components: (1) the physical phenomena of interest (sometimes called the process or plant), (2) sensors that send a time series y_k denoting the value of the physical measurement z_k at time k (e.g., the voltage at 3am is 120kV) to a controller, (3) based on the sensor measurements received y_k, the controller $\mathcal{K}(y_k)$ sends control commands u_k (e.g., open a valve by 10 %) to actuators, and (4) actuators that produce a physical change v_k in response to the control command (the actuator is the device that opens the valve).

A general security monitoring architecture for control systems that looks into the "physics" of the system needs an anomaly detection system that receives as inputs the sensor measurements y_k from the physical system and the control commands u_k sent to the physical system, and then uses them to identify any suspicious sensor or control commands is shown in Fig. 1.

2.2 Taxonomy

Anomaly detection is usually performed in two steps. First we need a model of the physical system that predicts the output of the system $\hat{y}_k$. The second step compares that prediction $\hat{y}_k$ to the observations y_k and then performs a statistical test on the difference. The difference between prediction and observation is usually called the **residual** r_k. We now present our new taxonomy for related work, based on four aspects: (1) physical model, (2) detection statistic, (3) metrics, and (4) validation.

Physical Model. The model of how a physical system behaves can be developed from physical equations (Newton's laws, fluid dynamics, or electromagnetic laws) or it can be learned from observations through a technique called *system identification* [4, 38]. In system identification one often has to use either Auto-Regressive Moving Average with eXogenous inputs (ARMAX) or linear state-space models. Two popular models used by the papers we survey are **Auto-Regressive (AR)** models and **Linear Dynamical State-space (LDS)** models.

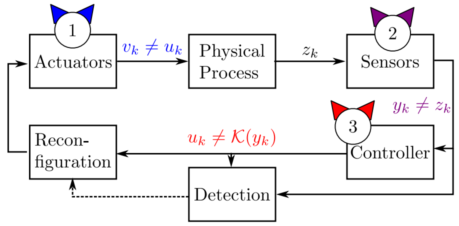


Figure 1: Different attack points in a control system: (1) Attack on the actuators (blue): $v_k \neq u_k$, (2) Attack on the sensors (purple): $y_k \neq z_k$, (3) Attack on the controller (red): $u_k \neq \mathcal{K}(y_k)$

An AR model for a time series y_k is given by

$$\hat{y}_{k+1} = \sum_{i=k-N}^{k} \alpha_i y_i + \alpha_0 \tag{1}$$

where α_i are obtained through system identification and y_i the last N sensor measurements. The coefficients α_i can be obtained by solving an optimization problem that minimizes the residual error (e.g., least squares) [37].

If we have inputs (control commands u_k) and outputs (sensor measurements y_k) available, we can use *subspace model identification* methods, producing LDS models:

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + \epsilon_k \\ y_k &= Cx_k + Du_k + e_k \end{aligned} \tag{2}$$

where A, B, C, and D are matrices modeling the dynamics of the physical system. Most physical systems are strictly causal and therefore $D = 0$ in general. The control commands $u_k \in \mathbb{R}^p$ affect the next time step of the state of the system $x_k \in \mathbb{R}^n$ and sensor measurements $y_k \in \mathbb{R}^q$ are modeled as a linear combination of these hidden states. e_k and ϵ_k are sensor and perturbation noise, and are assumed to be a random process with zero mean. To make a prediction, we i) first need y_k and u_k to obtain a *state estimate* $\hat{x}_{k+1}$ and ii) use the estimate to predict $\hat{y}_{k+1} = C\hat{x}_{k+1}$. A large body of work on power systems employs the second equation from Eq. (2) without the dynamic state equation. We refer to this special case of LDS used in power systems as **Static Linear State-space (SLS)** models.

Detection Statistic. If the observations we get from sensors y_k are significantly different from the ones we expect (i.e., if the residual is large) we generate an alert. A **Stateless** test, raises an alarm for every deviation at time k: i.e., if $|y_k - \hat{y}_k| = r_k \geq \tau$, where τ is a threshold.

In a **Stateful** test we compute an additional statistic S_k that keeps track of the historical changes of r_k (no matter how small) and generate an alert if $S_k \geq \tau$, i.e., if there is a persistent deviation across multiple time-steps. There are many tests that can keep track of the historical behavior of the residual r_k such as taking an average over a time-window, an exponential weighted moving average (EWMA), or using change detection statistics such as the non-parametric CUmulative SUM (CUSUM) statistic.

The nonparametric CUSUM statistic is defined recursively as $S_0 = 0$ and $S_{k+1} = (S_k + |r_k| - \delta)^+$, where $(x)^+$ represents $\max(0, x)$ and δ is selected so that the expected value of $|r_k| - \delta < 0$ under hypothesis H_0 (i.e., δ prevents S_k from increasing consistently under normal operation). An alert is generated whenever the statistic is greater than a previously defined threshold $S_k > \tau$ and the test is restarted with $S_{k+1} = 0$. The summary of our taxonomy for modeling the system and to detect an anomaly in the residuals is given in Fig. 2

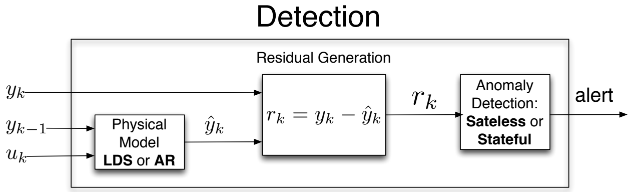


Figure 2: The detection block from Fig. 1 focusing on our taxonomy.

Metrics. An evaluation metric is used to determine the effectiveness of the physics-based attack detection algorithm. Popular evaluation metrics are the True Positive Rate (TPR) and the False Positive Rate (FPR)—the trade-off between these two numbers is called the Receiver Operating Characteristic (ROC) curve. Some papers just plot the residuals (without quantifying the TPR or FPR values), and other papers just measure the impact of attacks.

Validation. The experimental setting to validate proposals can use simulations, data from real-world operating systems, and testbeds. Testbeds can be classified as testbeds controlling a real-system or a testbed with Hardware-in-the-Loop (HIL) where part of the physical system is simulated in a computer. For our purposes a HIL testbed is similar to having pure simulations, because the model of the physical system is given by the algorithm running on a computer.

2.3 Limitations of Previous Work

There is a large variety of previous work but because of the diversity of domains (e.g., power systems, industrial control, and theoretical studies) and academic venues (e.g., security, control theory, and power systems conferences), the field has not been presented in a unified way with a common language that can be used to identify trends, alternatives, and limitations. Using our previously defined taxonomy, in this section we discuss previous work and summarize our results in Table 1.

The columns in Table 1 are arranged by conference venue (we assigned workshops to the venue that the main conference is associated with), we also assigned conferences associated with CPSWeek to control conferences because of the overlap of attendees to both venues. We make the following observations: (1) the vast majority of prior work use stateless tests; (2) most control and power grid venues use LDS (or their static counterpart SLS) to model the physical system, while computer security venues tend to use a variety of models, several of them are non-standard and difficult to replicate by other researchers; (3) there is no consistent metric or adversary model used to evaluate proposed attack-detection algorithms; and (4) no previous work has validated their work with all three options: simulations, testbeds and real-world data.

The first three observations (1-3) are related: while previous work has used different statistical tests (stateless vs. stateful) and models of the physical system to predict its expected behavior, so far they have not been compared against each other, and this makes it difficult to build upon previous work (it is impossible to identify best practices without a way to compare different proposals). To address this problem we propose a general-purpose evaluation metric in § 4 that leverages our stealthy adversary model, and then compare previously proposed methods. Our results show that while stateless tests are more popular in the literature, stateful tests are better to limit the impact of stealthy attackers. In addition, we show that LDS models are better than AR models, that AR models proposed in previous work can be improved by leveraging correlation among different signals, and that having an integral controller can limit the impact of stealthy actuation attacks.

To address point (4) we conduct experiments using all three options: a testbed with a real physical process under control § 5.1, real-world data § 5.2, and simulations § 5.3. We show the advantages and disadvantages of each experimental setup, and the insights each of these experiments provide.

3. MOTIVATING EXAMPLE

The testbed we use for our experiments is a room-size, water treatment plant consisting of 6 stages to purify raw water. The testbed has a total of 12 PLCs (6 main PLCs and 6 in backup configuration to take over if the main PLC fails). The general description of each stage is as follows: *Raw water storage* is the part of the process where raw water is stored and it acts as the main water buffer supplying water to the water treatment system. It consists of one tank, an on/off valve that controls the inlet water, and a pump that transfers the water to the ultra filtration (UF) tank. In *Pretreatment* the Conductivity, pH, and Oxidation-Reduction Potential (ORP) are measured to determine the activation of chemical dosing to maintain the quality of the water within some desirable limits. This stage is illustrated in Fig. 3 and will be used in our motivating example. *Ultra Filtration* is used to remove the bulk of the feed water solids and colloidal material by using fine filtration membranes that only allow the flow of small molecules. After the small residuals are removed by the UF system, the remaining chlorines are destroyed in the *Dechlorinization* stage, using ultraviolet chlorine destruction unit and by dosing a solution of sodium bisulphite. *Reverse Osmosis* (RO) system is designed to reduce inorganic impurities by pumping the filtrated and dechlorinated water with a high pressure. Finally, in *RO final product* stage stores the RO product (clean water).

Figure 3: Stage controlling the pH level.

Attacking the *pH* level. In this process, the water's *pH* level is controlled by dosing the water with Hydrochloric Acid (HCl). Fig. 4 illustrates the normal operation of the plant: if the *pH* sensor reports a level above 7.05, the PLC sends a signal to turn On the HCl pump, and if the sensor reports a level below 6.95, it sends a signal to turn it Off.

Table 1: Taxonomy of related work. Columns are organized by publication venue.

	[8] Bobba *et al.*	[54] Sandberg *et al.*	[59] Teixeira *et al.*	[6] Bai, Gupta	[46] Mo *et al.*	[44] Mo, Sinopoli	[7] Bai *et al.*	[43] Miao *et al.*	[23] Hou *et al.*	[16] Eyisi *et al.*	[45] Mo *et al.*	[50] Pasqualetti *et al.*	[61] Teixeira *et al.*	[31] Kwon *et al.*	[60] Teixeira *et al.*	[15] Do *et al.*	[1,2] Amin *et al.*	[56] Smith	[25] Kerns *et al.*	[33] Liang *et al.*	[20] Giani *et al.*	[13] Dan, Sandberg	[28] Kosut *et al.*	[26] Kim, Poor	[14] Davis *et al.*	[57] Sridhar, Govindarasu	[29] Koutsandria *et al.*	[40] Mashima *et al.*	[35,36] Liu *et al.*	[49] Parvania *et al.*	[34] Lin *et al.*	[55] Shoukry *et al.*	[21] Hadziosmanovic *et al.*	[10] Cardenas *et al.*	[67] Wang *et al.*	[42] McLaughlin	[53] Sajjad *et al.*	[65] Valente, Cardenas	[30] Krotofil *et al.*	[66] Vukovic, Dan	[47] Morrow *et al.*	[12] Cui *et al.*	[9] Carcano *et al.*	[22] Hei *et al.*	[27] Kiss *et al.*
Venue	Control																			Smart/Power Grid								Security												Misc.					
Detection Statistic																																													
stateless	●	●	●	-	-	-	●	●	●	◐	●	●	●	●	●	-	●	◐	●	-	●	●	●	●	●	-	●	-	●	◐	●	-	●	-	◐	◐	-	-	●	●	●	●	●	-	●
stateful	-	-	-	◐	⊛	⊛	-	-	-	-	-	-	-	-	-	●	-	-	-	⊛	-	-	-	-	-	⊛	-	●	-	-	-	⊛	-	●	-	-	●	●	●	-	-	●	-	⊛	-
Physical Model																																													
AR	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	●	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-	-	-
SLS	●	●	◐	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	●	●	●	●	●	◐	-	-	-	●	-	-	-	-	-	-	-	-	-	-	◐	◐	●	-	-	-
LDS	-	-	-	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	-	-	-	-	-	-	-	-	-	-	-	-	●	-	●	-	-	●	-	-	-	-	-	-	-	-
other	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	●	●	-	-	◐	◐	-	-	-	●	●	-	●	●	-	-	-	●	◐	●
Metrics*																																													
impact	-	●	-	●	-	-	●	-	●	●	-	●	●	●	●	-	-	-	●	●	-	●	-	●	-	-	●	●	●	-	●	-	-	-	-	-	●	-	-	●	-	●	-	●	-
statistic	-	-	●	-	●	-	-	●	●	-	-	●	●	●	●	-	●	-	-	●	-	-	●	-	-	-	●	-	●	-	-	-	-	-	-	-	-	●	●	●	-	●	-	-	●
TPR	-	-	-	-	●	●	-	-	-	-	●	-	-	-	-	●	-	-	-	-	●	-	●	-	-	●	-	-	-	-	-	●	●	-	●	-	-	-	-	-	-	-	●	-	-
FPR	-	-	-	-	●	-	-	-	-	-	●	-	-	-	-	●	-	-	-	-	-	-	●	-	-	●	-	●	-	-	-	●	-	-	●	-	-	-	-	-	-	-	●	-	-
Validation																																													
simulation	-	●	●	●	●	●	●	●	●	●	●	●	●	●	-	●	-	●	●	●	-	●	●	●	●	●	◐	-	●	-	●	-	-	●	●	-	●	-	●	●	●	●	-	-	●
real data	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	●	-	-	-	-	-	-	-	◐	●	-	●	-	-	-	-	●	-	-	-	-	●	-	-	-	-	-	●	-
testbed	-	-	-	-	-	-	-	-	-	-	-	-	-	-	●	-	-	-	●	-	-	-	-	-	-	-	-	-	-	◐	-	●	●	-	-	●	-	-	-	-	-	-	●	-	-

Legend: ●: feature considered by authors, ◐: feature assumed implicitly but exhibits ambiguity, ⊛: a windowed stateful detection method is used, *Evaluation options have been abbreviated in the table: Attack Impact, Statistic Visualization, True Positive Rate, False Positive Rate.

The wide oscillations of the *pH* levels occur because there is a delay between the control actions of the HCl pump, and the water *pH* responding to it.

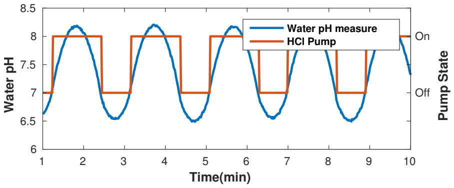


Figure 4: During normal operation, the water *pH* is kept in safe levels.

To detect attacks on the PLC, the pump or the sensor, we need to create a model of the physical system. While the system is nonlinear, let us first attempt it to model it as time-delayed LDS of order 2. The model is described by $pH_{k+1} = pH_k + u_{k-T_{delay}}$, where we estimate (by observing the process behavior) $u_{k-T_{delay}} = -0.1$ after a delay of 35 time steps after the pump is turned On, and 0.1 after a delay of 20 time steps after it is turned Off. We then compare the predicted and observed behavior, compute the residual, and apply a stateless, and a stateful test to the residual. If either of these statistics goes above a defined threshold, we raise an alarm.

We note that high or low *pH* levels can be dangerous. In particular, if the attacker can drive the *pH* below 5, the acidity of the water will damage the membranes of the *Ultra Filtration* and *Reverse Osmosis* stages, the pipes, and even sensor probes.

We launch a wired Man-In-The-Middle (MitM) attack between the field devices (sensors and actuators) and the PLC by injecting a malicious device in the EtherNet/IP ring of the testbed, given that the implementation of this protocol is unauthenticated. A detailed implementation of our attack is given in our previous work [64]. In particular, our MitM intercepts sensor values coming from the HCL pump and the *pH* sensor, and intercept actuator commands going to the HCl pump, to inject false sensor readings and commands sent to the PLC and HCl pump.

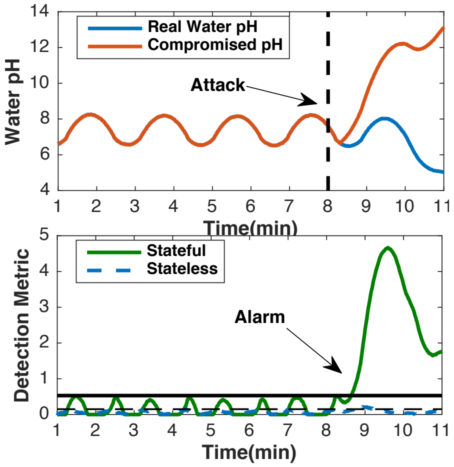


Figure 5: Attack to the *pH sensor*.

Our attack sends false sensor data to the PLC, faking a high *pH* level so the pump keeps running, and thus driving the acidity of the water to unsafe levels, as illustrated in Fig. 5. Notice that both, stateless and stateful tests detect this attack (each test has a different threshold set to main-

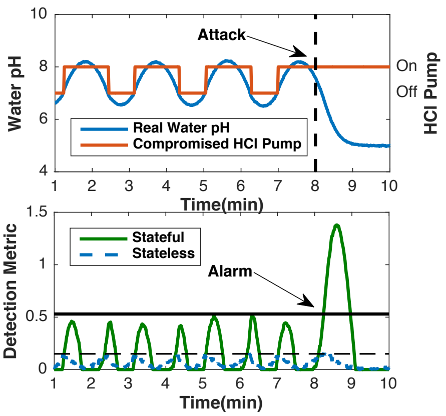


Figure 6: Attack to the pump *actuator*.

tain a probability of false alarm of 0.01). We also launched an attack on the pump (actuator). Here the pump ignores Off control commands from the PLC, and sends back messages stating that it is indeed Off, while in reality it is On. As illustrated in Fig. 6, only the stateful test detects this attack. We also launched several random attacks that were easily detected by the stateful statistic, and if we were to plot the ROC curve of these attacks, we would get 100% detection rate.

Observations. As we can see, it is very easy to create attacks that can be detected. Under these simulations we could initially conclude that our LDS model combined with the stateful anomaly detection are good enough; after all, they detected all attacks we launched. However, are these attacks enough to conclude that our LDS model is good enough? And if these attacks are not enough, then which types of attacks should we launch?

Notice that for any physical system, a sophisticated attacker can spoof deviations that follow relatively close the "physics" of the system while still driving the system to a different state. How can we measure the performance of our anomaly detection algorithm against these attacks? How can we measure the effectiveness of our anomaly detection tool if we assume that the attacker will always **adapt** to our algorithms and launch an undetected attack? And if our algorithms are not good enough, how can we design better algorithms? If by definition the attack is undetected, then we will always have a 0% true positive rate, therefore we need to devise new metrics to evaluate our systems.

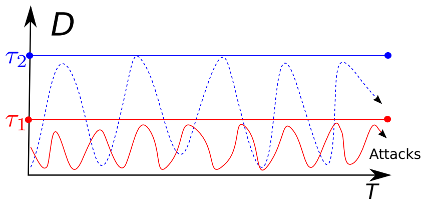


Figure 7: Our attacker adapts to different detection thresholds: If we select τ_2 the adversary launches an attack such that the detection statistic (dotted blue) remains below τ_2. If we lower our threshold to τ_1, the adversary selects a new attack such that the detection statistic (solid red) remains below τ_1.

4. A STRONGER ADVERSARY MODEL

We assume an attacker that has compromised a sensor (e.g. pH level in our motivating example) or an actuator (e.g. pump in our motivating example) in our system. We also assume that the adversary has complete knowledge of our system, i.e. she knows the physical model we use, the statistical test we use, and the thresholds we select to raise alerts. Given this knowledge, she generates a stealthy attack, where the detection statistic will always remain below the selected threshold.

While similar stealthy attacks have been previously proposed [13, 35, 36], in this paper we extend them for generic control systems including process perturbations and measurement noise, we force the attacks to remain stealthy against stateful tests, and also force the adversary to optimize the negative impact of the attack. In addition, we assume our adversary is **adaptive**, so if we lower the threshold to fire an alert, the attacker will also change the attack so that the anomaly detection statistic remains below the threshold. This last property is illustrated in Fig. 7.

Notice that this type of adaptive behavior is different from how traditional metrics such as ROC curves work, because they use the same attacks for different thresholds of the anomaly detector. On the other hand, our adversary model requires a new and unique (undetected) attack specifically tailored for every anomaly detection threshold. If we try to compute an ROC curve under our adversary model we would get a 0% detection rate because the attacker would generate a new undetected attack for every anomaly detection threshold.

This problem is not unique to ROC curves: most popular metrics for evaluating the classification accuracy of intrusion detection systems (like the intrusion detection capability, the Bayesian detection rate, accuracy, expected cost, etc.) are known to be a multi-criteria optimization problem between two fundamental trade-off properties: the false alarm rate, and the true positive rate [11], and as we have argued, using any metric that requires a true positive rate will be ineffective against our adversary model launching undetected attacks.

Observation. Most intrusion detection metrics are variations of the fundamental trade-off between false alarms and true positive rates [11], however, our adversary by definition will never be detected so we cannot use true positive rates (or variations thereof). Notice however that by forcing our adversary to remain undetected, we are effectively forcing her to launch attacks that follow closely the physical behavior of the system (more precisely, we are forcing our attacker to follow more closely our *Physical Model*), and by following closer the behavior of the system, then the attack impact is reduced: the attack needs to appear to be a plausible physical system behavior. So the trade-off we are looking for with this new adversary model is not one of *false positives* vs. *true positives*, but one between *false positives* and *the impact of undetected attacks.*

New Metric. To define precisely what we mean by *impact of undetected attack* we select one (or more) variables of interest (usually a variable whose compromise can affect the safety of the system) in the process we want to control–e.g., the pH level in our motivating example. The impact of the undetected attack will then be, how much can the attacker drive that value towards its intended goal (e.g., how much can the attacker lower the pH level while remaining undetected) per unit of time.

Therefore we propose a new metric consisting of the trade-

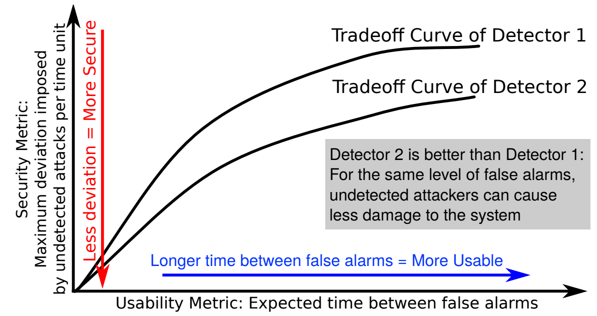

Security Metric:
Maximum deviation imposed
by undetected attacks per time unit
Less deviation = More Secure
Tradeoff Curve of Detector 1
Tradeoff Curve of Detector 2
Detector 2 is better than Detector 1:
For the same level of false alarms,
undetected attackers can cause
less damage to the system
Longer time between false alarms = More Usable
Usability Metric: Expected time between false alarms

Figure 8: Illustration of our proposed tradeoff metric. The y-axis is a measure of the maximum deviation imposed by undetected attacks per time unit Δ_X/TU, and the x-axis represents the expected time between false alarms $\mathbb{E}[T_{fa}]$. Anomaly detection algorithms are then evaluated for different points in this space.

off between the maximum deviation per time unit imposed by undetected attacks (y-axis) and the expected time between false alarms (x-axis). Our proposed trade-off metric is illustrated in Fig. 8, and its comparison to the performance of Receiver Operating Characteristic (ROC) curves against our proposed adversary model is illustrated in Fig. 9.

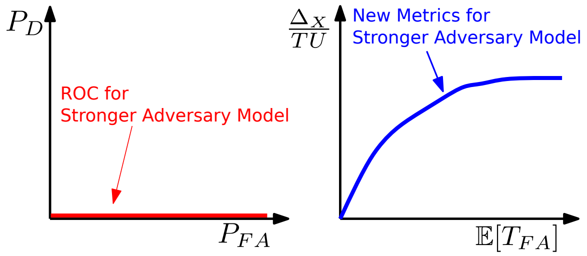


Figure 9: Comparison of ROC curves with our proposed metric: ROC curves are not a useful metric against a stealthy and adaptive adversary.

Notice that while the y-axis of our proposed metric is completely different to ROC curves, the x-axis is similar, but with a key difference: instead of using the probability of false alarms, we use instead the expected time between false alarms $\mathbb{E}[T_{fa}]$. This quantity has a couple of advantages over the false alarm rate: (1) it addresses the deceptive nature of low false alarm rates due to the base-rate fallacy [5], and (2) it addresses the problem that several anomaly detection statistics make a decision ("alarm" or "normal behavior") at non-constant time-intervals.

We now describe how to compute the y-axis and the x-axis of our proposed metric.

4.1 Computing the X and Y axis of Fig. 8

Computing Attacks Designed for the Y-axis of our Metric. The adversary wants to maximize the deviation of a variable of interest y_k (per time unit) without being detected. The true value of this variable is $y_k, y_{k+1}, \ldots, y_N$, and the attack starts at time k, resulting in a new observed time series $y^a_k, y^a_{k+1}, \ldots, y^a_N$. The goal of the attacker is to maximize the distance $\max_i ||y_i - y^a_i||$. Recall that in general y_k can be a vector of n sensor measurements, and that the attack y^a_k is a new vector where some (or all) of the sensor measurements are compromised.

An optimal greedy-attack (y^{a*}) at time $k \in [\kappa, \kappa_f]$ (where κ and κ_f are the initial and final attack times, respectively), satisfies the equation: $y^{a*}_{k+1} = \arg\max_{y^a_{k+1}} f(y^a_{k+1})$ (where $f(y^a_{k+1})$ is defined by the designer of the detection method to quantify the attack impact) subject to not raising an alert (instead of max it can be min). For instance, if $f(y^a_{k+1}) = ||y_{k+1} - y^a_{k+1}||$, the greedy attack for a stateless test is: $y^{a*}_{k+1} = \hat{y}_{k+1} \pm \tau$. The greedy optimization problem for an attacker facing a stateful CUSUM test becomes $y^{a*}_{k+1} = \max\{y^a_{k+1} : S_{k+1} \leq \tau\}$. Because $S_{k+1} = (S_k + r_k - \delta)$ the optimal attack is given when $S_k = \tau$, which results in $y^{a*}_{k+1} = \hat{y}_{k+1} \pm (\tau + \delta - S_k)$. For all attack times k greater than the initial time of attack κ, $S_k = \tau$ and $y^{a*}_{k+1} = \hat{y}_{k+1} \pm \ \delta$.

Generating undetectable **actuator attacks** is more difficult than **sensor attacks** because in several practical cases it is impossible to predict the outcome y_{k+1} with 100% accuracy, given the actuation attack signal v_k in Fig. 1. For our experiments when the control signal is compromised in § 5.3, we use the linear state space model from Eq. (2) to do a reverse prediction from the intended y^{a*}_{k+1} to obtain the control signal v_k that will generate that next sensor observation.

Computing the X-axis of our Metric. Most of the literature that reports false alarms uses the false alarm rate metric. This value obscures the practical interpretation of false alarms: for example a 0.1% false alarm rate depends on the number of times an anomaly *decision* was made, and the time-duration of the experiment: and these are variables that can be selected: for example a *stateful* anomaly detection algorithm that monitors the difference between expected $\hat{y}_k$ and observed y_k behavior has three options with every new observation k: (1) it can declare the behavior as *normal*, (2) it can generate an *alert*, (3) it can decide that the current evidence is inconclusive, and it can decide to take one more measurement y_{k+1}.

Because *the amount of time T that we have to observe the process and then make a decision is not fixed, but rather is a variable that can be selected*, using the false alarm rate is misleading and therefore we have to use ideas from *sequential detection theory* [24]. In particular, we use the average *time between false alarms* T_{FA}, or more precisely, the expected time between false alarms $\mathbb{E}[T_{FA}]$. We argue that telling security analysts that e.g., they should expect a false alarm every hour is a more direct and intuitive metric rather than giving them a probability of false alarm number over a decision period that will be variable if we use *stateful* anomaly detection tests. This way of measuring alarms also deals with the *base rate fallacy*, which is the problem where low false alarm rates such as 0.1% do not have any meaning unless we understand the likelihood of attacks in the dataset (the base rate of attacks). If the likelihood of attack is low, then low false alarm rates can be deceptive [5].

In all the experiments, the usability metric for each evaluated detection mechanism is obtained by counting the number of false alarms nFA for an experiment with a duration T_E under normal operation (without attack), so for each threshold τ we calculate the estimated time for a false alarm by $E[T_{fa}] \approx T_E/nFA$. Computing the average time between false alarms in the CUSUM test is more complicated than with the stateless test. In the CUSUM case, we need to compute the evolution of the statistic S_k for every threshold we test, because once S_k hits the threshold we have to reset it to zero.

Notice that while we have defined a specific impact for

Algorithm 1: Computing Y axis

```
Define $f(y^a_{k+1})$
Select $\tau_{set} = \{\tau_1, \tau_2, \ldots\}$, $\kappa$, $\kappa_f$, and
    $K_{set} = \{\kappa, \ldots, k_f - 1\}$
$\forall(\tau, k) \in \tau_{set} \times K_{set}$, find
    $y^{a*}_{k+1}(\tau) = \arg\max_{y^a_{k+1}} f(y^a_{k+1})$
        $s.t.$
        Detection Statistic $\leq \tau$
$\forall \tau \in \tau_{set}$, calculate
    $y - axis = \max_{k \in K_{set}} f(y^{a*}_{k+1}(\tau))$
```

Algorithm 2: Computing X axis

```
Observations $Y^{na}$ with no attacks of time-duration $T_E$
$\forall \tau \in \tau_{set}$, compute
    Detection Statistic: $D_S(Y^{na})$
    Number of false alarms: $nFA(D_S, \tau)$
    $x - axis = E[T_{fa}(\tau)] = T_E / nFA$
```

undetected attacks in our y-axis for clarity, we believe that designers who want to evaluate their system using our metric should define an appropriate *worst case undetected attack* optimization problem specifically for their system. In particular, the y-axis can be a representation of a cost function f of interest to the designer. There are a variety of metrics (optimization objectives) that can be measured such as the product degradation from undetected attacks, or the historical deviation of the system under attack $\sum_i |y_i - \hat{y}^a_i|$ or the deviation at the end of the attack $|y_N - \hat{y}^a_N|$, etc. A summary of how to compute the y-axis and the x-axis of our metric is given in Algorithms 1 and 2.

5. EXPERIMENTAL RESULTS

Table 2: Advantages and disadvantages of different evaluation setups.

Reliability of:	X-Axis	Y-Axis
Real Data		○
Testbed	◐	◐
Simulation	○	

= well suited, ◐ = partially suitable, ○ = least suitable

We evaluate anomaly detection systems under the light of our *Stronger Adversary Model* (see section § 4), using our new metrics in a range of test environments, with individual strengths and weaknesses (see Table 2). As shown in the table, real-world data allows us to analyze operational large-scale scenarios, and therefore it is the best way to test the x-axis metric $\mathbb{E}[T_{fa}]$. Unfortunately, real-world data does not give researchers the flexibility to launch attacks and measure the impact on all parts of the system. Such interactive testing requires the use of a dedicated physical testbed.

A physical testbed has typically a smaller scale than a real-world operational system, so the fidelity in false alarms might not be as good as with real data, but on the other hand, we can launch attacks. The attacks we can launch are, however, constrained because physical components and devices may suffer damage by attacks that violate the safety requirements and conditions for which they were designed for. Moreover, attacks could also drive the testbed to states that endanger the operator's and environment's safety. Therefore, while a testbed provides more experimental interaction than real data, it introduces safety constraints for launching attacks.

Simulations on the other hand, do not have these constraints and a wide variety of attacks can be launched. So our simulations will focus on attacks to actuators and demonstrate settings that cannot be achieved while operating a real-world system because of safety constraints. Simulations also allow us to easily change the control algorithms and to our surprise, we found that control algorithms have a big impact on the ability of our attacker to achieve good results in the y-axis of our metric. However, while simulations allow us to test a wide variety of attacks, the problem is that the false alarms measured with a simulation are not going to be as representative as those obtained from real data or from a testbed.

5.1 Physical Testbed (EtherNet/IP packets)

In this section, we focus on testbeds that control a real physical process, as opposed to testbeds that use a *Hardware-In-the-Loop* (HIL) simulation of the physical process. A HIL testbed is similar to the experiments we describe in § 5.3.

We developed an attacker who has complete knowledge of the physical behavior of the system and can manipulate EtherNet/IP packets and inject attacks. We now apply our metric to the experiments we started in section § 3.

Attacking pH Level. Because this system is highly nonlinear, apart from the simple physical model (LDS) of order 2 we presented in section § 3, we also applied a system identification to calculate higher order system models: an LDS model of order 20 and two nonlinear models (order 50 and 100) based on wavelet networks [52]. Fig. 10 shows the minimum pH achieved by the attacker after 4-minutes and against three different models. *Notice that the nonlinear models limited the impact of the stealthy attack by not allowing deviations below a pH of 5*, while our linear model (which was successful in detecting attacks in our motivating example) was not able to prevent the attacker from taking the pH below 5.

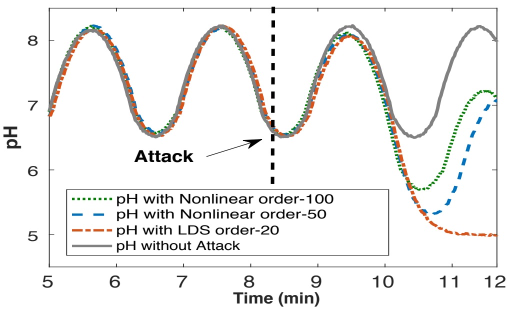


Figure 10: pH deviation imposed by greedy attacks while using stateful detection ($\tau = 0.05$) with both, LDS and nonlinear models.

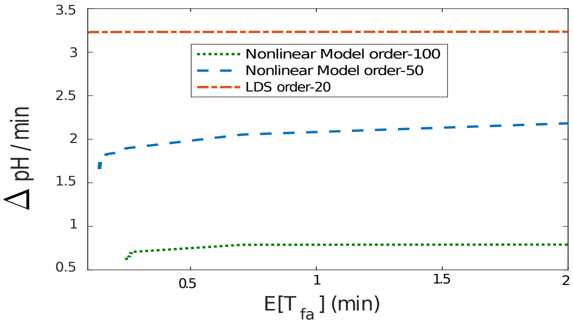


Figure 11: Comparison of LDS and nonlinear models to limit attack impact using our metric. Higher order nonlinear models perform better.

Fig. 11 illustrates the application of our proposed metric over 10 different undetected greedy attacks, each averaging 4 minutes, to evaluate the three system models used for detection. Given enough time, it is not possible to restrict a deviation of pH below 5. Nevertheless, for all $E[T_{fa}](min)$, the nonlinear model of order 100 performs better than the nonlinear model of order 50 and the LDS of order 20, limiting the impact of the attack per minute Δ_{pH}/min. It would take over 5 minutes for the attacker to deviate the pH below 5 without being detected using a nonlinear model of order 100, whereas it would take less than 3 minutes with the nonlinear of order 50 and the LDS of order 20.

5.1.1 *Attacking the Water Level*

Now we turn to another stage in our testbed. The goal of the attacker this time is to deviate the water level in a tank as much as possible until the tank overflows.

While in the pH example we had to use system identification to learn LDS and nonlinear models, the evolution of the water level in a tank is a well-known LDS system that can be derived from first principles. In particular, we use a mass balance equation that relates the change in the water level h with respect to the inlet Q^{in} and outlet Q^{out} volume of water, given by $Area\frac{dh}{dt} = Q^{in} - Q^{out}$, where $Area$ is the cross-sectional area of the base of the tank. Note that in this process the control actions for the valve and pump are On/Off. Hence, Q^{in} or Q^{out} remain constant if they are open, and zero otherwise. Using a time-discretization of 1 s, we obtain an LDS model of the form

$$h_{k+1} = h_k + \frac{Q_k^{in} - Q_k^{out}}{Area}.$$

Note that while this equation might look like an AR model, it is in fact an LDS model because the input $Q_k^{in} - Q_k^{out}$ changes over time, depending on the control actions of the PLC (open/close inlet or start/stop pump). In particular it is an LDS model with $x_k = h_k$, $u_k = [Q_k^{in}, Q_k^{out}]^T$, $B = [\frac{1}{Area}, -\frac{1}{Area}]$, $A = 1$, and $C = 1$.

Recall that the goal of the attacker is to deviate the water level in a tank as much as possible until the tank overflows. In particular, the attacker increases the water level sensor signal at a lower rate than the real level of water (Fig. 12) with the goal of overflowing the tank. A **successful attack** occurs if the PLC receives from the sensor a *High* water-level message (the point when the PLC sends a command to close the inlet), and at that point, the deviation (Δ) between the real level of water and the "fake" level (which just reached the High warning) is $\Delta \geq Overflow - High$. Fig. 12 shows three water level attacks with different increment rates, starting from the *Low* level setting and stopping at the *High* level setting, and their induced maximum Δ over the real level. Only attacks a_1 and a_2 achieve a successful overflow (only a_2 achieves a water spill), while a_3 deviates the water level without overflow. In our experiment, *High* corresponds to a water level of 0.8 m and *Low* to 0.5 m. Overflow occurs at 1.1 m. The testbed has a drainage system to allow attacks that overflow the tank.

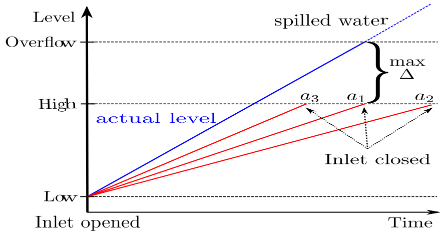


Figure 12: Impact of different increment rates on overflow attack. The attacker has to select the rate of increase with the lowest slope while remaining undetected.

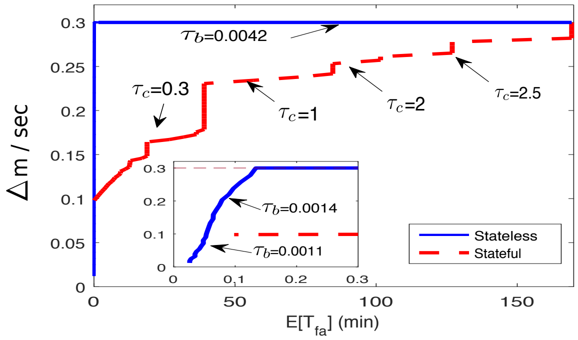


Figure 13: Comparison of stateful and stateless detection. At 0.3m the tank overflows, so stateless tests are not good for this use case. τ_b, τ_c correspond to the threshold associated to some $E[T_{fa}]$.

Because it was derived from "first principles", our LDS model is a highly accurate physical model of the system, so there is no need to test alternative physical models. However, we can combine our LDS model with a stateless test, and with a stateful test and see which of these detection tests can limit the impact of stealthy attacks.

In particular, to compute our metric we need to test stateless and stateful mechanisms and obtain the security metric that quantifies the impact Δ of undetected attacks for several thresholds τ. We selected the parameter $\delta = 0.002$ for the stateful (CUSUM) algorithm, such that the detection metric S_k remains close to zero when there is no attack. The usability metric is calculated for $T_E = 8$ h, which is the time of the experiment without attacks.

Fig. 13 illustrates the maximum impact caused by 20 different undetected attacks, each of them averaging 40 minutes. Even though the attacks remained undetected, the impact using stateless detection is such that a large amount of water can be spilled. Only for very small thresholds is it possible to avoid overflow, but it causes a large number of false alarms. On the other hand, stateful detection limits the impact of the adversary. Note that to start spilling water (i.e., $\Delta > 0.3\ m$) a large threshold is required. Clearly, selecting a threshold such that $E[T_{fa}] = 170\ min$ can avoid the spilling of water with a considerable tolerable number of false alarms.

In addition to attacking sensor values, we would like to analyze undetected actuation attacks. To launch attacks on the actuators (pumps) of this testbed, we would need to turn them On and Off in rapid succession in order try to maintain the residuals of the system low enough to avoid being detected. We cannot do this on real equipment because the pumps would get damaged. Therefore, we will analyze undetected actuator attacks with simulations (where equipment cannot be damaged) in § 5.3.

5.2 Large-Scale Operational Systems (Modbus packets)

We were allowed to place a network sniffer on a real-world operational large-scale water facility in the U.S. We collected more than 200GB of network packet captures of a system using the Modbus/TCP [63] industrial protocol. Our goal is to extract the sensor and control commands from this trace and evaluate and compare alternatives presented in the survey.

The network has more than 100 controllers, some of them with more than a thousand registers. In particular, 1) 95% of transmissions are Modbus packets and the rest 5% corresponds to general Internet protocols; 2) the trace captured 108 Modbus devices, of which one acts as central master, one as external network gateway, and 106 are slave PLCs; 3) of the commands sent from the master to the PLCs, 74% are *Read/Write Multiple Registers* (0x17) commands, 20% are *Read Coils* (0x01) commands, and 6% are *Read Discrete Inputs* (0x02) commands; and 4) 78% of PLCs count with 200 to 600 registers, 15% between 600 to 1000, and 7% with more than 1000.

We replay the traffic traces in packet capture (pcap) format and use Bro [51] to track the memory map of holding (read/write) registers from PLCs. We then use Pandas [68], a Python Data Analysis Library, to parse the log generated by Bro and to extract per PLC the time series corresponding to each of the registers. Each time series corresponds to a signal (y_k) in our experiments. We classify the signals as 91.5% *constant*, 5.3% *discrete* and 3.2% *continuous* based on the data characterization approach proposed to analyze Modbus traces [21] and uses AR models (as in Eq. (1)). We follow that approach by modeling the continuous time-series in our dataset with AR models. The order of the AR model is selected using the *Best Fit* criteria from the Matlab system identification toolbox [39], which uses unexplained output variance, i.e., the portion of the output not explained by the AR model for various orders [41].

Using the AR model, our first experiment centers on deciding which statistical detection test is better, a stateless test or the stateful CUSUM change detection test. Fig. 14 shows the comparison of stateless vs. stateful tests with our proposed metrics (where the duration of an undetected attack is 10 minutes). As expected, once the CUSUM statistic reaches the threshold $S_k = \tau$, the attack no longer has enough room to continue deviating the signal without being detected, and larger thresholds τ do not make a difference once the attacker reaches the threshold, whereas for the stateless test, the attacker has the ability to change the measurement by τ units at every time step.

Having shown that a CUSUM (stateful) test reduces the impact of a stealthy attack when compared to the stateless test we now show how to improve the AR physical model previously used by Hadziosmanovic et al. [21]. In particular, we notice that Hadziosmanovic et al. use an AR model *per signal*; this misses the opportunity of creating models of how multiple signals are correlated, creating correlated physical models will limit the impact of undetected attacks.

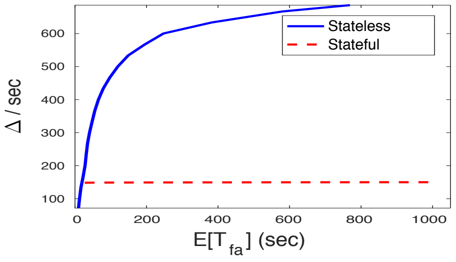


Figure 14: Stateful performs better than stateless detection: The attacker can send larger undetected false measurements for the same expected time to false alarms.

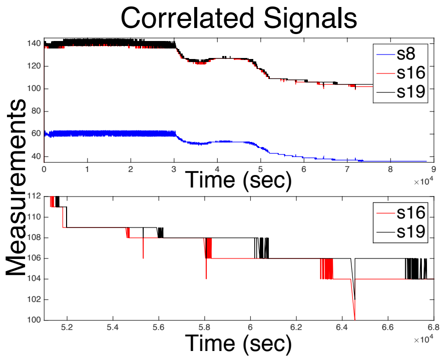


Figure 15: Three example signals with significant correlations. Signal S_{16} is more correlated with S_{19} than it is with S_8.

Spatial and Temporal Correlation. In an ideal situation the water utility operators could help us identify all control loops and spatial correlations of all variables (the water pump that controls the level of water in a tank etc.); however, this process becomes difficult to perform in a large-scale system with thousands of control and sensor signals exchanged every second; therefore we now attempt to find correlations empirically from our data. We correlate signals by computing the correlation coefficients of different signals $s_1, s_2, \cdots, s_N$. The correlation coefficient is a normalized variant of the mathematical covariance function: $\text{corr}(s_i, s_j) = \frac{\text{cov}(s_i,s_j)}{\sqrt{\text{cov}(s_i,s_i)\text{cov}(s_j,s_j)}}$ where $\text{cov}(s_i, s_j)$ denotes the covariance between s_i and s_j and correlation ranges between $-1 \leq \text{corr}(s_i, s_j) \leq 1$. We then calculate the *p-value* of the test to measure the significance of the correlation between signals. The *p-value* is the probability of having a correlation as large (or as negative) as the observed value when the true correlation is zero (i.e., testing the null hypothesis of no correlation, so lower values of p indicate higher evidence of correlation). We were able to find 8,620 correlations to be highly significant with $p = 0$.

Because corr(s_i, s_j) = corr(s_j, s_i) there are 4,310 unique significant correlated pairs. We narrow down our attention to corr$(s_i, s_j) > .96$. Fig. 15 illustrates three of the correlated signals we found. Signals s_{16} and s_{19} are highly correlated with corr$(s_{16}, s_{19}) = .9924$ while s_8 and s_{19} are correlated but with a lower correlation coefficient of corr$(s_8, s_{19}) = .9657$. For our study we selected to use signal s_8 and its most correlated signal s_{17} which are among the top most correlated signal pairs we found with corr$(S_8, S_{17}) = .9996$.

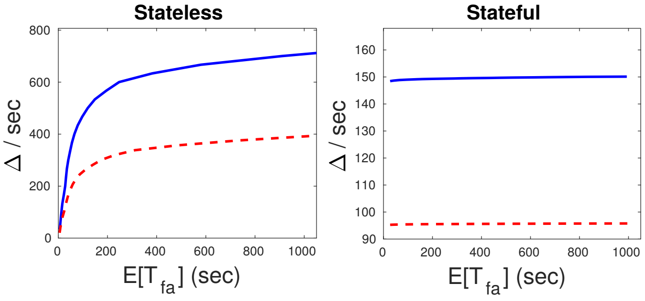


Figure 16: Using the defined metrics, we show how our new correlated AR models perform better (with stateless or stateful tests) than the AR models of independent signals.

Our experiments show that an AR model trained with correlated signals (see Fig. 16) is more effective in limiting the maximum deviation the attacker can achieve (assuming the attacker only compromises one of the signals). For that reason, we encourage future work to use correlated AR models rather than AR models of single signals.

5.3 Simulations of the Physical World

With simulations we can launch actuator attacks without the safety risk of damaging physical equipment. In particular, in this section we launch actuation attacks and show how the control algorithm used can significantly limit the impact of stealthy attackers. In particular we show that the Integrative part of a Proportional Integral Derivative (PID) control algorithm (or a PI or I control algorithm) can correct the deviation injected by the malicious actuator, and force the system to return to the correct operating state.

We use simulations of primary frequency control in the power grid as this is the scenario used by the Aurora attack [69]. Our goal is to maintain the frequency of the power grid as close as possible to 60Hz, subject to perturbations—i.e., changes in the Mega Watt (MW) demand by consumers—and attacks.

We assume that the attacker takes control of the actuators. When we consider attacks on a control signal, we need to be careful to specify whether or not the anomaly detection system can observe the false control signal. In this section, we assume the worst case: our anomaly detection algorithm cannot see the manipulated signal and indirectly observes the attack effects from sensors (e.g., v_k is controlled by the attacker, while the detection algorithm observes the valid u_k control signal, see Fig. 1).

Attacking a sensor is easier for our stealthy adversary because she knows the exact false sensor value $\hat{y}$ that will allow her to remain undetected while causing maximum damage. On the other hand, by attacking the actuator the attacker needs to find the input u_k that deviates the frequency enough, but still remains undetected. This is harder because even if the attacker has a model of the system, the output signal is not under complete control of the attacker: consumers can also affect the frequency of the system (by increasing or decreasing electricity consumption), and therefore they can cause an alarm to be generated if the attacker is not conservative. We assume the worst possible case of an omniscient adversary that knows how much consumption will happen at the next time-step (this is a conservative approach to evaluate the security of our system, in practice we expect the anomaly detection system to perform better because no attacker can predict the future).

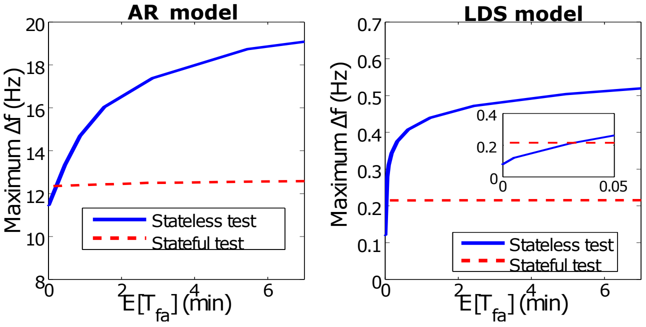


Figure 17: These figures show two things: (1) the stateful (CUSUM) test performs better than stateless tests when using AR (left) or LDS (right) models, and (2) LDS models perform an order of magnitude better than AR models (right vs left). Only for really small values of $\tau < \delta$ (0.04 minutes on average between false alarms), will the stateless test performs better than the stateful test.

We now evaluate all possible combinations of the popular *physical models* and *detection statistics* illustrated in Table 1. In particular we want to test AR models vs. LDS models estimated via system identification (SLS models do not make sense here because our system is dynamic) and stateless detection tests vs. stateful detection tests.

We launch an undetected actuator attack after 50 seconds using stateless and stateful detection tests for both: AR and LDS physical models. Our experiments show that LDS models outperform AR models, and that stateful models (again) outperform stateless models, as illustrated in Fig 17. These wide variations in frequency would not be tolerated in a real system, but we let the simulations continue for large frequency deviations to illustrate the order of magnitude ability from LDS models to limit the impact of stealthy attackers when compared to AR models.

Having settled for LDS physical models with CUSUM as the optimal combination of physical models with detection tests, we now evaluate the performance of different control algorithms, a property that has rarely been explored in our survey of related work. In particular, we show how Integrative control is able to correct undetected actuation attacks.

In particular we compare one of the most popular control algorithms: P control, and then we compare it to PI control. If the system operator has a P control of the form $u_k = Ky_k$, the attacker can affect the system significantly, as illustrated in Fig. 18. However, if the system operator uses a PI control, the effects of the attacker are limited: The actuator attack will tend to deviate the frequency signal, but this deviation will cause the controller to generate a cumulative compensation (due to the integral term) and because the LDS model knows the effect of this cumulative compensation, it is going to expect the corresponding change in the sensor measure-

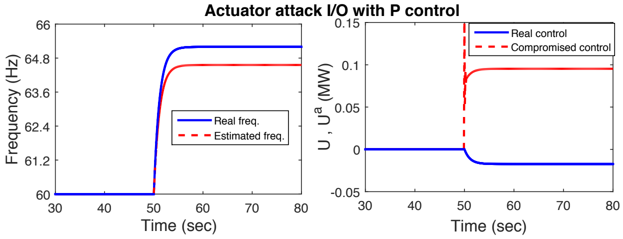


Figure 18: Left: The real (and trusted) frequency signal is increased to a level higher than the one expected (red) by our model of physical system given the control commands. Right: If the defender uses a P control algorithm, the attacker is able to maintain a large deviation of the frequency from its desired 60Hz set point.

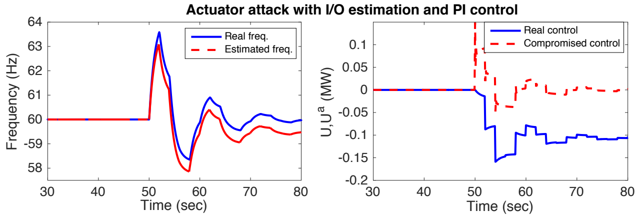


Figure 19: Same setup as in Fig. 18, but this time the defender uses a PI control algorithm: this results in the controller being able to drive the system back to the desired 60Hz operation point.

ment. As a consequence, to maintain the distance between the estimated and the real frequency below the threshold, the attack would have to decrease its action. At the end, the only way to maintain the undetected attack is when the attack is non-existent $u_k^a = 0$, as shown in Fig. 19.

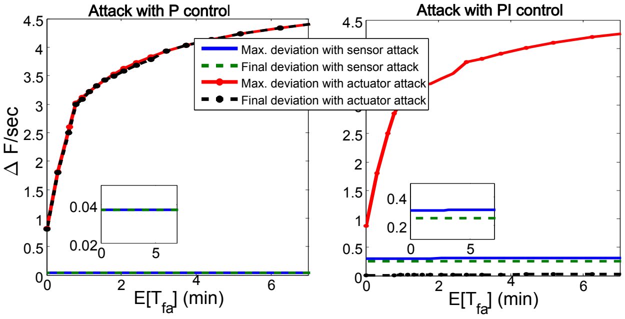


Figure 20: Differences between attacking sensors and actuators, and effects when the controller runs a P control algorithm vs. a PI control algorithm.

In all our previous examples with attacked sensors (except for the pH case), the worst possible deviation was achieved at the end of the attack, but for actuation attacks (and PI control), we can see that the controller is compensating the attack in order to correct the observed frequency deviation, and thus the final deviation will be zero: that is, the asymptotic deviation is zero, while the transient impact of the attacker can be high. Fig. 20 illustrates the difference between measuring the maximum final deviation of the state of the system achieved by the attacker, and the maximum temporary deviation of the state of the system achieved by the attacker.

As we can see, the control algorithm plays a fundamental role in how effective an actuation attack can be. An attacker that can manipulate the actuators at will can cause a larger frequency error but for a short time when we use PI control; however, if we use P control, the attacker can launch more powerful attacks causing long-term effects. On the other hand, attacks on sensors have the same long-term negative effects independent of the type of control we use (P or PI). Depending on the type of system, short-term effects may be more harmful than long-term errors. In our power plant example, a sudden frequency deviation larger than 0.5 Hz can cause irreparable damage on the generators and equipment in transmission lines (and will trigger protection mechanisms disconnecting parts of the grid). Small long-term deviations may cause cascading effects that can propagate and damage the whole grid.

While it seems that the best option to protect against actuator attacks is to deploy PI controls in all generators, several PI controllers operating in parallel in the grid can lead to other stability problems. Therefore often only the central Automatic Generation Control (AGC) implements a PI controller although distributed PI control schemes have been proposed recently [3].

Recall that we assumed the actuation attack was launched by an omniscient attacker that knows even the specific load the system is going to be subjected (i.e., it knows exactly how much will consumers demand electricity at every timestep, something not even the controller knows). For many practical applications, it will be impossible for the attacker to predict exactly the consequence of its actuation attack due to model uncertainties (consumer behavior) and random perturbations. As such, the attacker has a non-negligible risk of being detected when launching actuation attacks when compared to the 100% certainty the attacker has of not being detected when launching sensor attacks. In practice, we expect that an attacker that would like to remain undetected using actuation attacks will behave conservatively to accommodate for the uncertainties of the model, and thus we expect that the maximum transient deviation from actuation attacks will be lower.

6. CONCLUSIONS

6.1 Findings

We introduced theoretical and practical contributions to the growing literature of physics-based attack detection in control systems. Our literature review from different domains of expertise unifies disparate terminology, and notation. We hope our efforts can help other researchers refine and improve a common language to talk about physics-based attack detection across computer security, control theory, and power system venues.

In particular, in our survey we identified a lack of unified metrics and adversary models. We explained in this paper the limitations of previous metrics and adversary models, and proposed a novel stealthy and adaptive adversary model, together with its derived intrusion detection metric, that can be used to study the effectiveness of physics-based attack-detection algorithms in a systematic way.

We validated our approaches in multiple setups, including: a room-size water treatment testbed, a real large-scale operational system managing more than 100 PLCs, and simulations of primary frequency control in the power grid. We showed in Table 2 how each of these validation setups has advantages and disadvantages when evaluating the x-axis and y-axis of our proposed metric.

One result we obtained across our testbed, real operational systems, and simulations, is the fact that stateful tests perform better than stateless tests. This is in stark contrast to the popularity of stateless detection statistics as summarized in Table 1. We hope our paper motivates more implementations of stateful instead of stateless tests in future work.

We also show that for a stealthy actuator attack, PI controls play an important role in limiting the impact of this attack. In particular we show that the Integrative part of the controller corrects the system deviation and forces the attacker to have an effective negligible impact asymptotically.

Finally, we also provided the following novel observations: (1) finding spatio-temporal correlations of Modbus signals has not been proposed before, and we showed that these models are better than models of single signals, (2) while input/output models like LDS are popular in control theory, they are not frequently used in papers published in security conferences, and we should start using them because they perform better than the alternatives, unless we deal with a highly-nonlinear model, in which case the only way to limit the impact of stealthy attacks is to estimate nonlinear physical models of the system, and (3) we show why launching undetected attacks in actuators is more difficult than in sensors.

6.2 Discussion and Future Work

While physics-based attack detection can improve the security of control systems, there are some limitations. For example, in all our experiments the attacks affected the residuals and anomaly detection statistics while keeping them below the thresholds; however, there are special cases where depending on the power of the attacker or the characteristics of the plant, the residuals can remain zero (ignoring the noise) while the attacker can drive the system to an arbitrary state. For example, if the attacker has control of all sensors and actuators, then it can falsify the sensor readings so that our detector believes the sensors are reporting the expected state given the control signal, while in the meantime, the actuators can control the system to an arbitrary unsafe condition.

Similarly, some properties of the physical systems can also limit us from detecting attacks. For example, systems vulnerable to zero-dynamics attacks [61], unbounded systems [62], and highly non-linear or chaotic systems [48].

Finally, one of the biggest challenges for future work is the problem of how to respond to alerts. While in some control systems simply reporting the alert to operators can be considered enough, we need to consider automated response mechanisms in order to guarantee the safety of the system. Similar ideas in our metric can be extended to this case, where instead of measuring the false alarms, we measure the impact of a false response. For example, our previous work [10] considered switching a control system to open-loop control whenever an attack in the sensors was detected (meaning that the control algorithm will ignore sensor measurements and will attempt to estimate the state of the system based only on the expected consequences of its control commands). As a result, instead of measuring the false alarm rate, we focused on making sure that a reconfiguration triggered by a false alarm would never drive the system to an unsafe state. Therefore maintaining safety under both, attacks and false alarms, will need to take priority in the study of any automatic response to alerts.

Acknowledgments

The work at UT Dallas was supported by NIST under award 70NANB14H236 from the U.S. Department of Commerce and by NSF CNS-1553683. The work of Justin Ruths at SUTD was supported by grant NRF2014NCR-NCR001-40 from NRF Singapore. H. Sandberg was supported in part by the Swedish Research Council (grant 2013-5523) and the Swedish Civil Contingencies Agency through the CERCES project. We thank the iTrust center at SUTD for enabling the experiments on the SWaT testbed.

Disclaimer

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

7. REFERENCES

[1] S. Amin, X. Litrico, S. Sastry, and A. Bayen. Cyber security of water SCADA systems; Part I: Analysis and experimentation of stealthy deception attacks. *IEEE Transactions on Control Systems Technology*, 21(5):1963–1970, 2013.

[2] S. Amin, X. Litrico, S. Sastry, and A. Bayen. Cyber security of water SCADA systems; Part II: Attack detection using enhanced hydrodynamic models. *IEEE Transactions on Control Systems Technology*, 21(5):1679–1693, 2013.

[3] M. Andreasson, D. V. Dimarogonas, H. Sandberg, and K. H. Johansson. Distributed pi-control with applications to power systems frequency control. In *Proceedings of American Control Conference (ACC)*, pages 3183–3188. IEEE, 2014.

[4] K. J. Åström and P. Eykhoff. System identification—a survey. *Automatica*, 7(2):123–162, 1971.

[5] S. Axelsson. The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information and System Security (TISSEC)*, 3(3):186–205, 2000.

[6] C.-z. Bai and V. Gupta. On Kalman filtering in the presence of a compromised sensor : Fundamental performance bounds. In *Proceedings of American Control Conference*, pages 3029–3034, 2014.

[7] C.-z. Bai, F. Pasqualetti, and V. Gupta. Security in stochastic control systems : Fundamental limitations and performance bounds. In *Proceedings of American Control Conference*, 2015.

[8] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye. Detecting false data injection attacks on DC state estimation. In *Proceedings of Workshop on Secure Control Systems*, volume 2010, 2010.

[9] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta. A multidimensional critical state analysis for detecting intrusions in SCADA systems. *IEEE Transactions on Industrial Informatics*, 7(2):179–186, 2011.

[10] A. A. Cardenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the ACM symposium on information, computer and communications security*, pages 355–366, 2011.

[11] A. A. Cárdenas, J. S. Baras, and K. Seamon. A framework for the evaluation of intrusion detection systems. In *Proceedings of Symposium on Security and Privacy*, pages 77–91. IEEE, 2006.

[12] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer. Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions. *Signal Processing Magazine, IEEE*, 29(5):106–115, 2012.

[13] G. Dán and H. Sandberg. Stealth attacks and protection schemes for state estimators in power systems. In *Proceedings of Smart Grid Commnunications Conference (SmartGridComm)*, October 2010.

[14] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine. Power flow cyber attacks and perturbation-based defense. In *Proceedings of Conference on Smart Grid Communications (SmartGridComm)*, pages 342–347. IEEE, 2012.

[15] V. L. Do, L. Fillatre, and I. Nikiforov. A statistical method for detecting cyber/physical attacks on SCADA systems. In *Proceedings of Control Applications (CCA)*, pages 364–369. IEEE, 2014.

[16] E. Eyisi and X. Koutsoukos. Energy-based attack detection in networked control systems. In *Proceedings of the Conference on High Confidence Networked Systems (HiCoNs)*, pages 115–124, New York, NY, USA, 2014. ACM.

[17] N. Falliere, L. O. Murchu, and E. Chien. W32. stuxnet dossier. White paper, Symantec Corp., Security Response, 2011.

[18] D. Formby, P. Srinivasan, A. Leonard, J. Rogers, and R. Beyah. Who's in control of your control system? Device fingerprinting for cyber-physical systems. In *Network and Distributed System Security Symposium (NDSS), Feb*, 2016.

[19] R. M. Gerdes, C. Winstead, and K. Heaslip. CPS: an efficiency-motivated attack against autonomous vehicular transportation. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pages 99–108. ACM, 2013.

[20] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla. Smart grid data integrity attacks: characterizations and countermeasures π. In *Proceedings of Smart Grid Communications Conference (SmartGridComm)*, pages 232–237. IEEE, 2011.

[21] D. Hadžiosmanović, R. Sommer, E. Zambon, and P. H. Hartel. Through the eye of the PLC: semantic security monitoring for industrial processes. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pages 126–135. ACM, 2014.

[22] X. Hei, X. Du, S. Lin, and I. Lee. PIPAC: patient infusion pattern based access control scheme for wireless insulin pump system. In *Proceedings of INFOCOM*, pages 3030–3038. IEEE, 2013.

[23] F. Hou, Z. Pang, Y. Zhou, and D. Sun. False data injection attacks for a class of output tracking control systems. In *Proceedings of Chinese Control and Decision Conference*, pages 3319–3323, 2015.

[24] T. Kailath and H. V. Poor. Detection of stochastic processes. *IEEE Transactions on Information Theory*, 44(6):2230–2231, 1998.

[25] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys. Unmanned aircraft capture and control via gps spoofing. *Journal of Field Robotics*, 31(4):617–636, 2014.

[26] T. T. Kim and H. V. Poor. Strategic protection against data injection attacks on power grids. *IEEE Transactions on Smart Grid*, 2(2):326–333, 2011.

[27] I. Kiss, B. Genge, and P. Haller. A clustering-based approach to detect cyber attacks in process control systems. In *Proceedings of Conference on Industrial Informatics (INDIN)*, pages 142–148. IEEE, 2015.

[28] O. Kosut, L. Jia, R. Thomas, and L. Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *Proceedings of Smart Grid Commnunications Conference (SmartGridComm)*, October 2010.

[29] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParland, and A. Scaglione. A hybrid network IDS for protective digital relays in the power transmission grid. In *Proceedings of Smart Grid Communications (SmartGridComm)*, 2014.

[30] M. Krotofil, J. Larsen, and D. Gollmann. The process matters: Ensuring data veracity in cyber-physical systems. In *Proceedings of Symposium on Information, Computer and Communications Security (ASIACCS)*, pages 133–144. ACM, 2015.

[31] C. Kwon, W. Liu, and I. Hwang. Security analysis for cyber-physical systems against stealthy deception attacks. In *Proceedings of American Control Conference*, pages 3344–3349, 2013.

[32] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. *Security & Privacy, IEEE*, 9(3):49–51, 2011.

[33] J. Liang, O. Kosut, and L. Sankar. Cyber attacks on ac state estimation: Unobservability and physical consequences. In *Proceedings of PES General Meeting*, pages 1–5, July 2014.

[34] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. K. Iyer. Semantic security analysis of SCADA networks to detect malicious control commands in power grids. In *Proceedings of the workshop on Smart energy grid security*, pages 29–34. ACM, 2013.

[35] Y. Liu, P. Ning, and M. K. Reiter. False data injection attacks against state estimation in electric power grids. In *Proceedings of ACM conference on Computer and communications security (CCS)*, pages 21–32. ACM, 2009.

[36] Y. Liu, P. Ning, and M. K. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):13, 2011.

[37] L. Ljung. *The Control Handbook*, chapter System Identification, pages 1033–1054. CRC Press, 1996.

[38] L. Ljung. *System Identification: Theory for the User*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2 edition, 1999.

[39] L. Ljung. *System Identification Toolbox for Use with MATLAB*. The MathWorks, Inc., 2007.

[40] D. Mashima and A. A. Cárdenas. Evaluating electricity theft detectors in smart grid networks. In

Research in Attacks, Intrusions, and Defenses, pages 210–229. Springer, 2012.

[41] I. MathWorks. Identifying input-output polynomial models. www.mathworks.com/help/ident/ug/identifying-input-output-polynomial-models.html, October 2014.

[42] S. McLaughlin. CPS: Stateful policy enforcement for control system device usage. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pages 109–118, New York, NY, USA, 2013. ACM.

[43] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas. Coding sensor outputs for injection attacks detection. In *Proceedings of Conference on Decision and Control*, pages 5776–5781, 2014.

[44] Y. Mo and B. Sinopoli. Secure control against replay attacks. In *Proceedings of Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 911–918. IEEE, 2009.

[45] Y. Mo, S. Weerakkody, and B. Sinopoli. Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Systems*, 35(1):93–109, 2015.

[46] Y. L. Mo, R. Chabukswar, and B. Sinopoli. Detecting integrity attacks on SCADA systems. *IEEE Transactions on Control Systems Technology*, 22(4):1396–1407, 2014.

[47] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye. Topology perturbation for detecting malicious data injection. In *Proceedings of Hawaii International Conference on System Science (HICSS)*, pages 2104–2113. IEEE, 2012.

[48] E. Ott, C. Grebogi, and J. A. Yorke. Controlling chaos. *Physical review letters*, 64(11):1196, 1990.

[49] M. Parvania, G. Koutsandria, V. Muthukumary, S. Peisert, C. McParland, and A. Scaglione. Hybrid control network intrusion detection systems for automated power distribution systems. In *Proceedings of Conference on Dependable Systems and Networks (DSN)*, pages 774–779, June 2014.

[50] F. Pasqualetti, F. Dorfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *Automatic Control, IEEE Transactions on*, 58(11):2715–2729, Nov 2013.

[51] V. Paxson. Bro: a system for detecting network intruders in real-time. *Computer networks*, 31(23):2435–2463, 1999.

[52] S. Postalcioglu and Y. Becerikli. Wavelet networks for nonlinear system modeling. *Neural Computing and Applications*, 16(4-5):433–441, 2007.

[53] I. Sajjad, D. D. Dunn, R. Sharma, and R. Gerdes. Attack mitigation in adversarial platooning using detection-based sliding mode control. In *Proceedings of the ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC)*, pages 43–53, New York, NY, USA, 2015. ACM. http://doi.acm.org/10.1145/2808705.2808713.

[54] H. Sandberg, A. Teixeira, and K. H. Johansson. On security indices for state estimators in power networks. In *Proceedings of Workshop on Secure Control Systems*, 2010.

[55] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava. PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1004–1015, New York, NY, USA, 2015. ACM.

[56] R. Smith. A decoupled feedback structure for covertly appropriating networked control systems. In *Proceedings of IFAC World Congress*, volume 18, pages 90–95, 2011.

[57] S. Sridhar and M. Govindarasu. Model-based attack detection and mitigation for automatic generation control. *Smart Grid, IEEE Transactions on*, 5(2):580–591, 2014.

[58] R. Tan, V. Badrinath Krishna, D. K. Yau, and Z. Kalbarczyk. Impact of integrity attacks on real-time pricing in smart grids. In *Proceedings of the SIGSAC conference on Computer & communications security (CCS)*, pages 439–450. ACM, 2013.

[59] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry. Cyber security analysis of state estimators in electric power systems. In *Proceedings of Conference on Decision and Control (CDC)*, pages 5991–5998. IEEE, 2010.

[60] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson. Attack models and scenarios for networked control systems. In *Proceedings of the conference on High Confidence Networked Systems (HiCoNs)*, pages 55–64. ACM, 2012.

[61] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. Revealing stealthy attacks in control systems. In *Proceedings of Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1806–1813. IEEE, 2012.

[62] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. A secure control framework for resource-limited adversaries. *Automatica*, 51:135–148, 2015.

[63] The Modbus Organization. Modbus application protocol specification, 2012. Version 1.1v3.

[64] D. Urbina, J. Giraldo, N. Tippenhauer, and A. Cárdenas. Attacking fieldbus communications in ics: Applications to the swat testbed. In *Proceedings of the Singapore Cyber-Security Conference (SG-CRC), Singapore*, volume 14, pages 75–89, 2016.

[65] J. Valente and A. A. Cardenas. Using visual challenges to verify the integrity of security cameras. In *Proceedings of Annual Computer Security Applications Conference (ACSAC)*. ACM, 2015.

[66] O. Vuković and G. Dán. On the security of distributed power system state estimation under targeted attacks. In *Proceedings of the Symposium on Applied Computing*, pages 666–672. ACM, 2013.

[67] Y. Wang, Z. Xu, J. Zhang, L. Xu, H. Wang, and G. Gu. SRID: State relation based intrusion detection for false data injection attacks in SCADA. In *Proceedings of European Symposium on Research in Computer Security (ESORICS)*, pages 401–418. Springer, 2014.

[68] Pandas: Python data analysis library. http://pandas.pydata.org, November 2015.

[69] M. Zeller. Myth or reality—does the aurora vulnerability pose a risk to my generator? In *Proceedings of Conference for Protective Relay Engineers*, pages 130–136. IEEE, 2011.

Device-Level Jitter as a Probe of Ultrafast Traps in High-k MOSFETs

D. Veksler, J. P. Campbell, J. Zhong,[1] H. Zhu,[1] C. Zhao,[1] K. P. Cheung
NIST, 100 Bureau Dr., Gaithersburg, MD 20899, USA. Dmitry.veksler@nist.gov
[1]IMECAS, China

***Abstract*—A methodology for the evaluation of ultra-fast interfacial traps, using jitter measurements as a probe, is developed. This methodology is applied to study the effect of PBTI stress on the density of ultra-fast electron traps (with 500 ps to 5 ns characteristic capture/emission times) in a high-k/Si nMOSFET. It is shown, that in spite of an observed increase of timing jitter after PBTI stress, this increase may not be correlated with an increasing density of interface traps. Rather, it is solely caused by a V_T shift which simply decreases the output signal amplitude. The results indicate that ultra-fast (presumably interface) traps may not be affected by PBTI stress.**

***Index Terms*—D_{it}. jitter, high-K MOS, Interface characterization.**

I. INTRODUCTION

Timing jitter, manifested as a deviation of signal timing edges from their "correct" positions, is always an undesirable factor in electronics and telecommunications as it leads to corruption of signaling intervals. These jitter-induced errors impose limitations on the operating speed of modern integrated circuits. For the case of discrete MOSFETs, charge trapping and detrapping by fast traps is one of the possible origins of jitter. Fig. 1 illustrates the mechanistic description of jitter caused by electron trapping at the defects in the gate dielectric stack.

Previously, we developed a methodology to measure the jitter of a single device at realistic circuit speeds in response to BTI stress [1,2]. In this study, we apply similar techniques to probe fast electron traps (defects in the gate stack) in Si/high-k nMOSFETs. Using this approach, we attribute PBTI-induced jitter increase to a V_T shift, with seemingly no noticeable generation of fast electron traps in the devices under investigation.

II. EXPERIMENT

The experimental set-up is shown in Fig. 2. High-k/Si nMOSFETs with 2 nm HfO_2/0.8 nm SiO_2 gate stacks were used (30 μm X 100 nm). A user-defined sequence of ultra-fast pulses with variable widths and intervals between them was applied to the gate terminal of the device under study, while the drain terminal followed by a 50 ohm load resistor was held at constant voltage $V_d \approx 1$ V. The high-speed pattern generator used in the experiment had fixed rise and fall times ≈25 ps. Fast rise an fall times are essential for high resolution jitter measurements. The pattern generator clock rate was set to 2 GBit/s, the maximum clock rate at which the device response was not strongly affected by an RC delay (originating from device parasitics). The amplitude of the pulses were chosen to be high enough to open the device during the pulse (**on**-time interval), and to keep the device channel closed in between the pulses (**off**-time interval). The output drain current response was measured using a fast sampling oscilloscope and visualized using an eye diagram representation. Random fluctuations of the number of filled fast traps in the device under study after each **on/off** sequence should cause a variation in the device threshold voltage, and thus, should result in a distribution of transistor turn-**on/off** timing edges – jitter.

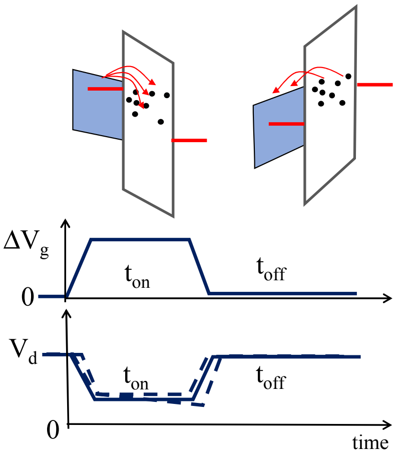


Figure 1. Schematic of trap kinetics during **on** (MOSFET channel is open) and **off** (MOSFET channel is closed) periods of the gate pulse sequence. Different numbers of traps are filled after each **t_{on}** and **t_{off}** interval causing V_T variation, and as a result, jitter of the output signal (dashed lines in the bottom panel).

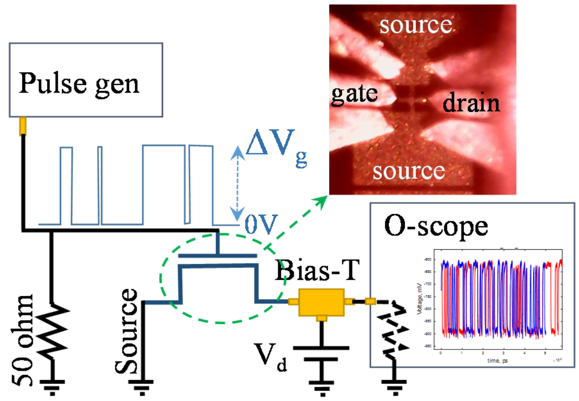


Figure 2. Experimental set-up. Device layout is designed to minimize parasitics. For these devices, the maximum data rate is 2 GBit/s. The experimental system is capable of 20 GBit/s characterizations.

U.S. Government work not protected by U.S. copyright

Veksler, Dmitry; Campbell, Jason; Cheung, Kin; Zhong, J.; Zhu, H.; Zhao, C.
"Device-Level Jitter as a Probe of Ultrafast Traps in High-k MOSFETs."
Paper presented at the 2016 IEEE International Reliability Physics Symposium, Pasadena, CA, Apr 17-Apr 21, 2016.

III. Results and Discussion

It was shown earlier [1,2] that a sequence of pulses of fixed width fired with fixed duty cycle, i.e. a signal pattern generated by a ring oscillator (RO), commonly used for jitter evaluation, does not allow one to confidently measure stress-related increase of jitter in a MOSFET. Involving numerical Monte Carlo simulations of trap charging/discharging kinetics, we discovered that driving the MOS transistor's gate with a RO pattern would not be an efficient way to produce jitter associated with filling/emptying traps at the oxide/channel interface. To maximize variation of the number of filled traps in the device at the time of each timing edge, it is beneficial to use a pseudo-random input signal pattern. (The details about simulations and results of the evaluation of the method sensitivity will be published elsewhere.) Pseudo-random binary bit sequence (PRBS) is well known in telecommunications [3].

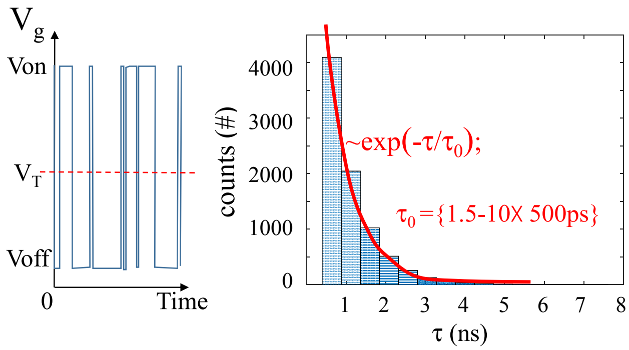


Figure 3. Generated pseudo-random (PRBS) input gate patterns with t_{on} (and t_{off}) following a Poisson distribution. With characteristic time τ_0 ranging from 750 ps to 5 ns to probe different traps through the oxide thickness.

For example, PRBS-15 consists of $2^{15} - 1$ bits, with **on** and **off** bits repeated in a random order, forming $\mathbf{t_{on}}$ and $\mathbf{t_{off}}$ intervals of random lengths. The distributions of numbers of repeating bits of the same value in the PRBS follow a Poisson distribution. Employing input signal patterns with different characteristic parameter, τ_0, (see Fig. 3) of the Poisson distribution of τ_{ON} and τ_{OFF} in our experiment, we measured jitter of rising and falling edges of the output signal at different signal levels (Fig. 4). In our experiment, τ_0 was changed in range from 750 ps up to 5 ns and was kept the same for distributions of both $\mathbf{t_{on}}$ and $\mathbf{t_{off}}$ interval lengths. The length of the pattern (16384 bits) and the number of pattern repetitions (4 times) taken for the jitter analysis is a tradeoff between the desired time resolution, the depth of the available oscilloscope memory, and the number of desired timing edges in the pattern. The latter should be sufficient to obtain statistically significant jitter distributions. It is worth noting that measuring jitter at different signal levels results in higher confidence in analyzing jitter distributions; this approach makes the analysis at least partially immune to any stress induced changes of the shape of the output signal. Note that purposeful variations of the PRBS characteristic times, τ_0, effectively varies the defect profiling range and can be a useful experimental tool to identify defects contributions to jitter, their characteristic capture and emission times, and location within the oxide stack.

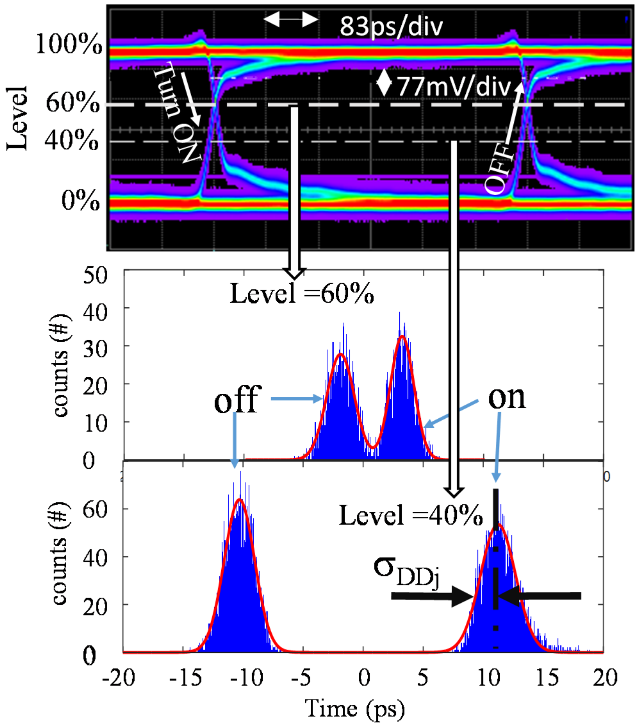


Figure 4. Representative experimental results show an eye diagram representation of the transistor output signal obtained using 2 GBit/s PRBS input signal (τ_0 = 750 ps, T = 300 K, $V_{dd} \cong 1.0$ V, and $V_T = 0.3$ V). The bottom panel illustrates the distribution of timing edge positions in the output signal measured at different signal levels for both the rising and falling edges. The dispersion, σ_{DDj}, in each distribution is used as a figure of merit to quantify the jitter.

The described methodology was applied to evaluate the generation of fast electron traps during PBTI stress in a MOSFET with a high-k gate stack. Devices under investigation were stressed at room temperature by applying +1.9 V to the gate while drain, source, and substrate were grounded. The stress was interrupted to perform jitter measurements. In an effort to remove recoverable degradation from consideration, all terminals were held at 0 V for a time period equal to the stress duration prior to each jitter measurement.

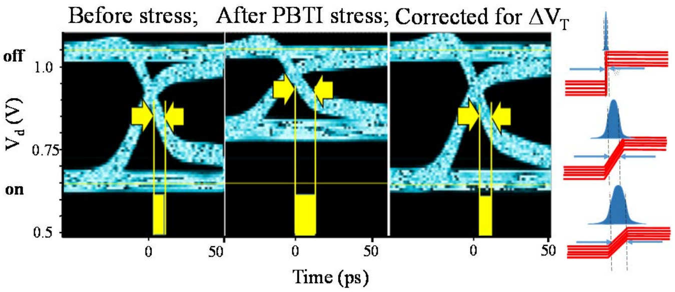
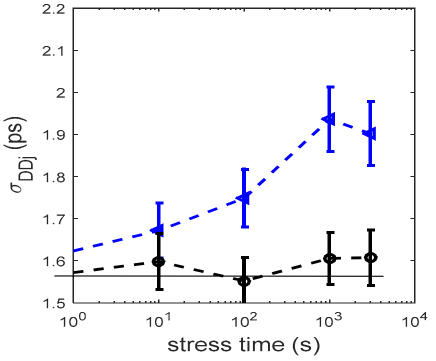


Figure 5. The left panel illustrates the pre- and post- PBTI eye diagrams as measured using a PRBS (τ_0 = 750 ps) input gate waveform. PBTI stress: 4000 s @ $V_{G,stress}$ = +1.9 V, $V_d = V_s = V_{sub} = 0$ V, T = 300 K). The PBTI induced V_T shift necessarily reduces the output signal amplitude and subsequently increases σ_{DDj}. However, a simple correction of the eye diagram for the V_T shift ($\Delta V_g = \Delta V_{g0} + \Delta V_T$) completely compensates the increase of the timing jitter. The right panel schematically illustrates how a reduction in signal amplitude necessarily causes an increase in measured jitter.

Fig. 5 (right panel) shows representative eye diagrams of the output drain signal before and after stress, obtained using a PRBS gate pattern with $\tau_0 = 750$ ps. The stress introduces the expected increase in jitter of both the **on** and **off** timing edges.

However, more detailed analysis did not relate the observed increase of the timing jitter with an increase of the interface trap density. After PBTI stress, reduction of the amplitude of the output signal from the MOSFETs under investigation was observed. The increase in measured jitter after stress was attributed to the stress related reduction of the output signal amplitude. The left panel of Fig. 5 schematically illustrates how a reduction in signal amplitude causes an increase in measured jitter. While the experimental rise and fall times of the input gate signal are kept the same, the V_T shift-induced reduction of output amplitude, ΔV_d, causes a reduction of the measured $d\Delta V_d/dt$ slope, and thus, increases jitter. After the amplitude of the input signal was increased to compensate for the stress-induced V_T shift ($\Delta V_g = \Delta V_{g0} + \Delta V_T$), the stress-induced increase of timing jitter, $\Delta\sigma_{DDj} = \sigma_{DDj}(t_{stress}) - \sigma_{DDj}(0)$, was completely compensated (Fig. 6). I.e. the observed stress induced jitter increase was strongly linked to a more permanent V_T shift and had very little to do with the generation of new fast traps in the device under study.



.

Figure 6. Jitter (σ_{DDj}) of the transistor output signal rising edge vs. PBTI stress time (V_{stress} = 1.9 V. T = 300 K). Jitter is measured using a PRBS pattern with τ_0=4.5 ns, at the signal level = 50% of the output signal amplitude. The blue dotted line reports the as measured jitter distributions (ΔV_G = 1.2 V). The black line is obtained by correcting for V_T shift after each stress.

We note that this increased jitter derived from the output signal amplitude reduction will impact the device timing and presumably the circuit timing, if introduced into a circuit, regardless of the origin of the increase. However, it is beneficial to know the physical mechanism responsible for the discussed increase of timing jitter during stress, as well as the reversibility of the jitter increase, and its connection with the specific types of defects in the device gate stack.

Pseudo-random bit patterns with different characteristic times, τ_0, were used in the experiment. If an input signal pattern with a longer τ_0 was used, one would expect to observe a contribution to jitter from larger numbers of traps, including traps located further away from the Si/SiO$_2$ interface. Fig. 7 shows the measured dependence of σ_{DDj} versus τ_0 before and after stress, and after increasing the input signal amplitude to compensate for the stress-induced increase of the device threshold voltage, V_T. The curves in Fig. 7 show very little dependence on τ_0. The seeming independence of jitter versus τ_0 implies that increasing average time intervals (**t$_{on}$** and **t$_{off}$**) do not necessarily cause an interaction of channel electrons with the larger numbers of traps. This may be an indication that fast traps contributing to jitter at the 2 Gbt/s rate have characteristic response times shorter than 750 ps – the shortest value of $\boldsymbol{\tau_0}$ used in the experiment.

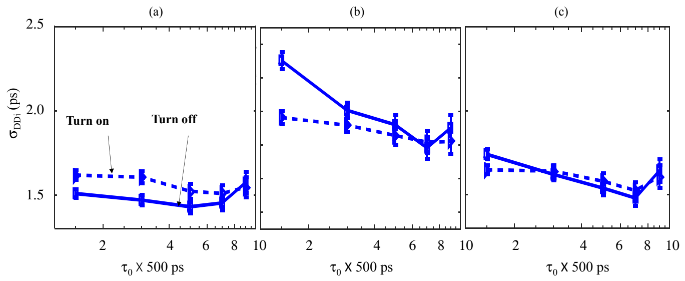


Figure 7. Jitter (σ_{DDj}) of the turn-on (dashed) and turn-off (solid) edges of the transistor output signal vs. the characteristic pattern distribution times (τ_0). These measurements are shown for both 50 % signal level. (a) Before stress. (b) After 4 ks PBTI stress (c) After stress, but corrected for V_T shift. The V_T corrected post PBTI jitter returns to the pre-stress levels.

IV. Conclusion

We develop a methodology to quantify ultra-fast (presumably interface) traps using jitter measurements as a probe. This methodology was applied to study the timing impact of PBTI stress in high-k/Si nMOSFETs (500 ps to 5 ns scale). It is shown that PBTI stress does increase the observed jitter, but that this increase is solely caused by a more permanent V_T shift, which decreases the output signal amplitude. More interestingly, our results indicate that PBTI does not cause detectable increase of the density of fast interface traps. This observation is in line with the literature reports stating that, contrarily to NBTI, PBTI stress does not create new fast defects at the Si/SiO$_2$ interface [4,5].

On the other hand, the evolution of MOSFET technology from SiO$_2$/poly-Si, to high-k/metal gate, and to III-V/high-k, has seen the level of acceptable interface defect density increase. This functions to enhance the significance of timing jitter moving forward. Thus, augmenting typical reliability data with circuit speed jitter measurements results in more complete understanding to optimize fabrication processes.

The developed methodology can be used for the evaluation of the interface quality and quantification of fast interface traps in MOSFET and HEMT devices, built using different technologies and material systems. It can be used to study the interface degradation induced by different type of stresses, including radiation effects.

References

1. G. F. Jiao, J.W. Lu, J.P. Campbell, J.T. Ryan, K.P. Cheung, C.D. Young, G. Bersuker, "Device-Level Experimental Observations of NBTI-Induced Random Timing Jitter"

IEEE Transactions on Device and Materials Reliability, vol.14(4), pp.972-977, 2014.

2. Jiwu Lu, G. Jiao, C. Vaz, J.P. Campbell, J.T. Ryan, K.P. Cheung, G. Bersuker, C. Young, "PBTI-Induced Random Timing Jitter in Circuit-Speed Random Logic". *IEEE Transactions on Electron Devices*, vol.61(11), pp.3613-3618, 2014.
3. Hervé Sizun and P.de Fornel *Radio Wave Propagation for Telecommunication Applications (Signals and Communication Technology)*, Springer; 2005 edition. ISBN-13: 978-3540407584.
4. M. Cho, Jae-Duk Lee, M. Aoulaiche, B. Kaczer, P. Roussel, T. Kauerauf, R. Degraeve, J. Franco, L.-Å. Ragnarsson, and G. Groeseneken. "Insight into N/PBTI mechanisms in sub-1-nm-EOT devices.", IEEE Transactions on Electron Devices, vol. 59(8), pp.2042-2048, 2012.
5. D. Veksler, G. Bersuker, M.B. Watkins, A. Shluger, "Activation of electrically silent defects in the high-k gate stacks". *IEEE International Reliability Physics Symposium,* 5B. 3.1-5B. 3.7, 2014.

This is an authors' format preprint. The final article was published in
Proc. SPIE 9778 (2016) 977809.

Virtual rough samples to test 3D nanometer-scale scanning electron microscopy stereo photogrammetry

J.S. Villarrubia, V.N. Tondare, and A.E. Vladár
Engineering Physics Division, Physical Measurements Laboratory, National Institute of Standards and Technology,[†] Gaithersburg, MD, USA 20899

ABSTRACT

The combination of scanning electron microscopy for high spatial resolution, images from multiple angles to provide 3D information, and commercially available stereo photogrammetry software for 3D reconstruction offers promise for nanometer-scale dimensional metrology in 3D. A method is described to test 3D photogrammetry software by the use of virtual samples—mathematical samples from which simulated images are made for use as inputs to the software under test. The virtual sample is constructed by wrapping a rough skin with any desired power spectral density around a smooth near-trapezoidal line with rounded top corners. Reconstruction is performed with images simulated from different angular viewpoints. The software's reconstructed 3D model is then compared to the known geometry of the virtual sample. Three commercial photogrammetry software packages were tested. Two of them produced results for line height and width that were within close to 1 nm of the correct values. All of the packages exhibited some difficulty in reconstructing details of the surface roughness.

Keywords: critical dimension (CD), dimensional metrology, model-based metrology, scanning electron microscopy (SEM), simulation, stereo photogrammetry, surface roughness, virtual sample

1. INTRODUCTION

With the introduction of non planar memory and logic devices beginning at the 22 nm node, semiconductor electronic devices began to have significant functional dependence on vertical dimensions of their structures. For FinFET or Tri-Gate transistor architectures, for example, the size of the conducting gate channel depends on the height of the fin. Structure height, wall angles, and sidewall roughness join width as critical process variables.[1]

In a scanning electron microscope (SEM) image, the lateral dimensions are spatial. The vertical dimension is an intensity related to the backscattered or secondary electron yield. The yield variation carries spatial information that can be retrieved with the help of a model that relates yield to shape.[2,3] Alternatively, tilting the sample permits a new image in which the vertical axis of the former image has a component in the new lateral direction. The change in lateral separation of features (known as disparity) is a function of tilt angles and the height difference of the features. Stereo photogrammetry (by which we mean estimation of 3D coordinates from sets of two or more images) may be used to reconstruct the 3D sample. Piazzesi described the mathematics of such reconstruction for SEM in 1973.[4] Others have looked extensively into various measuring and instrument errors, their avoidance, and their effect on the quality of reconstruction.[5-8]

There are beginning to be a large number of options for software to determine 3D sample shape from multiple views. At the time of this writing, 58 are listed in the Wikipedia article on "Comparison of photogrammetry software." When the purpose of 3D reconstruction is not merely an artistically pleasing rendering, but rather quantitative accurate measurement, how is one to judge the adequacy of software? In this paper we adopt the approach of using a virtual sample to assess software performance. By a virtual sample, we mean a mathematical description of an object that does not exist in reality. We make images of the object from different angles using the JMONSEL[3] simulator, much as one would make measurements of a real object in an actual SEM. These images then become the inputs to the stereo photogrammetry software. A disadvantage of this approach is that it does not test contributions of the instrument to measurement errors. For

[†] Contributions of the National Institute of Standards and Technology are not subject to copyright in the United States.

this reason, it is not a complete test; such errors must be assessed in other ways. The advantage of the approach is that the true sample shape is known with mathematical accuracy, a level that measurement errors make impossible to replicate in real samples at the nanometer scale relevant for features of interest in semiconductor electronics applications. This makes it possible for software designers to determine whether an algorithm strategy—more noise filtering or less, the method of discovery of homologous points in images of the input set, approximation A vs. approximation B—improves not only the appearance but the accuracy of the result.

The virtual sample was made rough, which permitted photogrammetry software to locate a high density of homologous points in image sets. We purchased three commercial software packages that advertise their use with SEM. We designate these A, B, and C, intentionally leaving them otherwise unspecified. We used these to reconstruct the sample shape. The center profile of the reconstructed shape was compared to the corresponding true profile from the virtual sample in order to determine reconstruction errors. The purpose of this sampling of available software is to learn something about the current state of the art for such reconstruction, as judged by measurement errors in the height, width, and roughness of our virtual specimen. Different software packages exhibit different levels of performance and perform better for some measurements than others. Our results demonstrate by example that useful things can be learned by this technique. We anticipate that such data sets will also be useful to software developers who wish to improve the reconstruction accuracy of their algorithms.

In Sec. 2 we describe our method for constructing a roughness-wrapped virtual sample with a desired power spectral density, representation of the sample in a form suitable for SEM simulation, and the simulation in JMONSEL from a series of different angular viewpoints. In Sec. 3 we describe the 3D reconstruction results with our software packages and compare them to the true sample shape. In Sec. 4 we discuss the significance of the results of this comparison.

2. ROUGHNESS-WRAPPED VIRTUAL SAMPLE

Generation of images to be used as input to the 3D reconstruction software was performed in several steps: (1) A rough surface was generated with the desired power spectral density (PSD). Roughness in this surface was all in the z direction (normal to the substrate). (2) This surface was wrapped around a smooth line. (3) The wrapping sometimes results in surface self-intersections (“collisions”) at inside corners. These collisions were resolved. (4) The collision-resolved, wrapped surface was represented as an intersection of three height maps. This form is recognized by JMONSEL, our image simulation software. (5) Images of the height-map-represented virtual sample were simulated at a sequence of tilt angles.

2.1 Generation of rough surface with desired power spectral density

Our algorithm to generate a rough surface proceeds in these steps:

1. We create a 2D array with the desired dimensions and populate it with unit amplitude “white noise” (white, that is, up to the array’s Nyquist frequency): normally distributed random numbers with mean 0 and variance 1.
2. We take the fast Fourier transform (FFT) of that array. The result is a complex-valued array, $\boldsymbol{Z}$ such that $\boldsymbol{Z}_{jk} = \boldsymbol{A}_{jk}\exp(i\Phi_{jk})$, where $\boldsymbol{A}$ and Φ are real-valued amplitude and phase arrays. By definition, the two-sided power spectral density of $\boldsymbol{Z}$ is the array with elements $(\boldsymbol{A}_{jk})^2$. Even though “white” implies equal amplitudes at all frequencies, the amplitudes (the elements $\boldsymbol{A}_{jk}$) are only equal *on average*. The equality is statistical, not rigorous in each realization of random noise.
3. Suppose our desired power spectral density is stored in array $\boldsymbol{P}$. Here we have a choice. If we want our generated surface to have exactly PSD $= \boldsymbol{P}$, we replace $\boldsymbol{A}$ with $\sqrt{\boldsymbol{P}}$ to form $\boldsymbol{Z}'_{jk} = \sqrt{\boldsymbol{P}_{jk}}\exp(i\Phi_{jk})$. If our application is better served by retaining the statistical variation of PSD realizations, we form instead the matrix $\boldsymbol{Z}'$ with elements $\boldsymbol{Z}'_{jk} = \sqrt{\boldsymbol{P}_{jk}}\boldsymbol{Z}_{jk}$. These options either replace or scale $\boldsymbol{Z}$’s original on-average flat, white-noise, PSD. Because $\boldsymbol{P}$ is a PSD and hence real valued, either option leaves unaltered the random phases generated in step 2.
4. We form the inverse FFT of $\boldsymbol{Z}'$. This is our desired rough surface.

Methods similar to this were recently reviewed by Mack[9]. If the statistical PSD option is chosen at step 3, the method is similar (possibly equivalent) to that of Thoros[10].

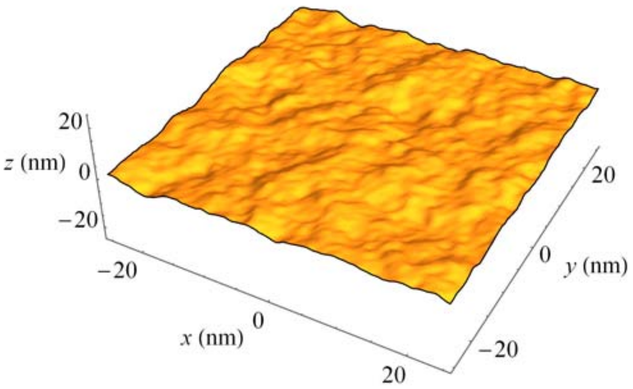


FIG. 1. A subset of the generated rough sample skin with root mean square 1 nm roughness and 15 nm correlation length.

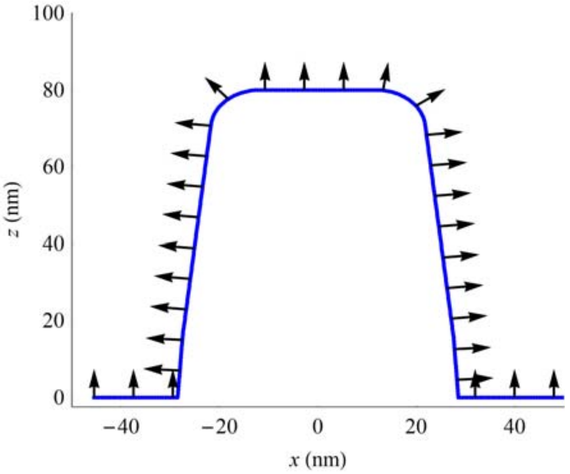


FIG. 2. A profile of the smooth, near-trapezoidal line around which the rough skin was wrapped. The arrows indicate local normals to the surface.

The desired PSD required for step 3 is specified as a 2D array of squared amplitudes. As such it is quite general, and need not be expressible in a simple analytical form. It could, for example, be chosen equal to the measured PSD of an actual sample. However, for the present application we chose to construct the array from Palasantzas's isotropic analytical form[11] for the PSD:

$$P(k) = \frac{4\pi\alpha\sigma^2\xi^2}{(1 + k^2\xi^2)^{1+\alpha}} \tag{1}$$

The leading constant factor in the PSD depends on one's choice of Fourier transform convention and whether the PSD is 1-sided or 2-sided. The version in Eq. 1 follows Zhao et al.[12] This PSD expression has parameters σ^2 for roughness variance, ξ for lateral correlation length, and α for roughness exponent. To keep them realistic we adopted values $\xi = 15$ nm and $\alpha = 1$ close to those obtained by fitting this expression to the PSD estimated from an image of a rough semiconductor industry sample available to us. We used $\sigma = 1$ nm. Equation 1was used to generate values to populate the PSD array, ***P***, for step 3 of the above procedure. Then step 4 produced our rough surface, a representative section of which is shown in Fig. 1.

2.2 Wrapping the sample

Our underlying sample shape is the smooth line shown in Fig. 2. It is an 80 nm tall line, 50 nm wide at half-height, wider on the bottom than the top, with sidewalls 3º from the vertical and 10 nm top corner radii. This represents the smooth average shape around which the rough "skin" described in the previous section must be wrapped. The skin consists of vertical (*z*) displacements (initially with $\sigma = 2$ nm) at equal intervals in *x* and in *y*. To wrap our shape we must discretize our smooth surface into a series of (*x*, *y*, *z*) coordinates at equal distances (arc length) along the surface, i.e., in the direction parallel to the local surface, not necessarily the *x* direction. Each of these points must then be displaced by an amount dictated by the corresponding point in the skin, but in a direction along the local surface normal, as indicated by the arrows in Fig. 2.

2.3 Collision resolution

Sometimes (e.g., near the bottom corners in the figure) these displacements cause one part of the surface to cross another part. If $p_i = (x_i, z_i)$ and p_{i+1} are adjacent points (same *y* value) along a roughened profile, we check whether the line segment that joins them intersects each of the other line segments, from p_j and p_{j+1} for all $j > i$. If any such intersections are found, the collision of the two affected segments can be resolved by reducing the displacements of their 4 endpoints to some fraction *f* ($0 \le f < 1$) of their original values. We use the largest value of *f* that resolves the collision. This may simply propagate the collision to a neighboring line segment. The procedure of checking and resolving collisions is therefore iterated until all collisions are resolved. At this point all displacements were further reduced by an additional factor of 2, yielding a surface roughness just under 1/2 the original value, for $\sigma = 1$ nm . A point cloud rendering of the resulting virtual sample is shown in Fig. 3.

2.4 Representation as an intersection of height maps

Electron trajectory simulations are necessary in order to produce simulated images of the virtual sample, but the surface point cloud representation described in the previous section is insufficient for that purpose. The simulator needs to assign scattering properties to volumes, and those volumes must be bounded by surfaces. Intersection of an electron's path with a bounding surface signals the transition to a new volume with possibly different scattering properties. The points in the point cloud lie on the boundary, but it remains to specify the surfaces that connect the points and the volumes that these surfaces bound. For this reason the point cloud representation was converted to a representation in terms of height maps.

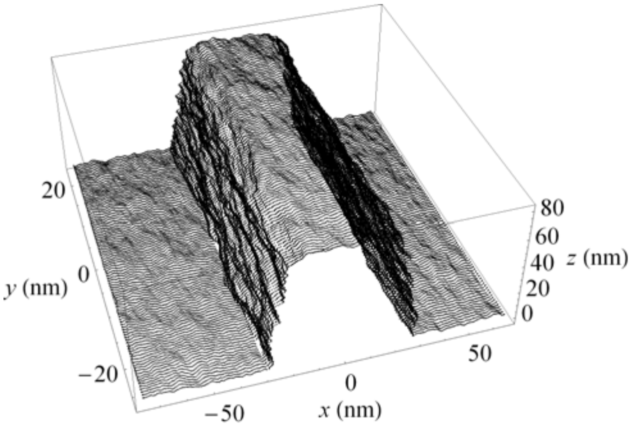


FIG. 3. Point cloud rendering of the virtual sample. Details in the right edge are obscured because there is no hidden surface removal.

A basic height map in the JMONSEL SEM simulator[3] that we used is a 2D array of z values, equally spaced in x and y. Consider one "cell" of this array, defined as the 4 points at positions (i, j), (i+1, j), (i, j+1), and (i+1, j+1). These 4 points define two triangular surfaces, one with vertices (x_i, y_j, z_{ij}), (x_{i+1}, y_j, $z_{i+1,j}$), and (x_i, y_{j+1}, $z_{i,j+1}$), the other with vertices (x_{i+1}, y_{j+1}, $z_{i+1,j+1}$), (x_{i+1}, y_j, $z_{i+1,j}$), and (x_i, y_{j+1}, $z_{i,j+1}$). Beyond the borders of the explicitly specified portion of the height map, i.e., to the left, right, above, or below in the x-y plane, the heights are considered to remain constant at the last specified value. The union of the surfaces from all the cells forms a surface that partitions space into two volumes: a lower one defined as the inside and an upper one defined to be outside. A cut at constant y through our virtual sample (with roughness exaggerated for clearer illustration) is indicated by the thin line in Fig. 4a. A cut at the same y through a corresponding height map is indicated by the thick line. The height map is constructed by dividing the desired interval into regularly spaced x values, $\{x_i\}$. For each x_i we find all intervals in the point cloud (thin line) that contain this x_i, interpolate the corresponding z for each such interval, and associate the maximum of these z values with that x_i. At most places, the virtual sample surface shown in Fig. 4a is single-valued and the height map very closely approximates it. (Errors are only those from interpolation, and may be made as small as we wish by making the interval between x_i small enough.) At the sidewalls, however, the roughness makes our virtual sample reentrant. At such locations, the higher parts of the sample shadow the lower parts, as is evident in the figure. The height map contains or bounds the sample, but in some places more tightly than others.

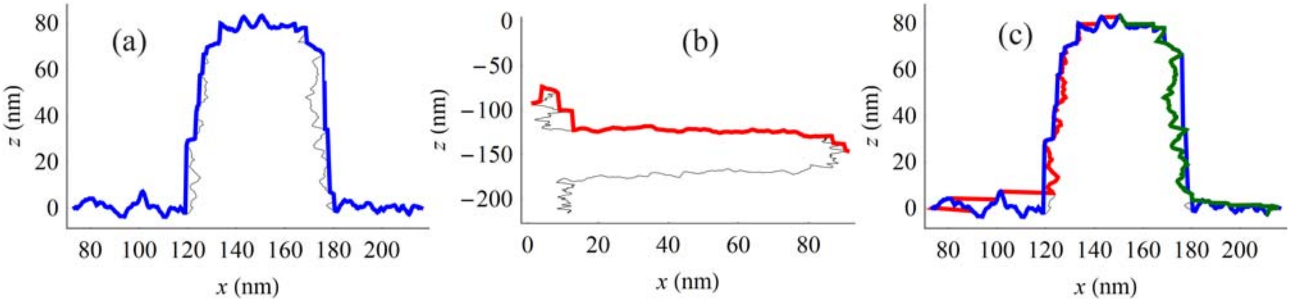


FIG. 4. Schematic of the representation of a sample by a combination of height maps. In all panels the sample is indicated by the thin line and its height map approximation by the thick line. (a) A height map in the sample's ordinary orientation forms an outer bound. (b) Another height map with the sample rotated 87º to the right, giving a better approximation of the left sidewall. (c) The intersection of 3 height maps (the 3rd from a rotation 87º to the left, not shown) after each was returned to the ordinary orientation.

The sample representation is improved by taking advantage of transformations and set operations that can be performed on height maps. The virtual sample was rotated 87º to the right as shown in Fig. 4b. A second height map, indicated again by the thicker line, was generated in this orientation, and then rotated 87º to the left, returning it to the original orientation. A third height map (not shown) was also formed, this time with the line rotated 87º to the left to expose the other sidewall, followed once again by the opposite rotation. Since each of these represents an outer bound on the sample, their intersection also represents an outer bound, in this case a noticeably tighter one (Fig. 4c). This intersection of three height maps was used to represent the sample in JMONSEL.

2.5 Simulation of SEM images

We used JMONSEL to import the height map representation of the virtual sample and produce images of the same location at sample tilts from –85° to 85º at 5º intervals. For each image, 10 000 electrons at 500 eV were raster scanned across 241 × 101 pixels, each of which had size 0.5 nm × 0.5 nm. Electron landing positions were normally distributed around the target position with standard deviation 0.5 nm. Electrons with energy between 0 eV and 50 eV that escaped to a hemispherical collector above the sample were counted and converted to a proportial intensity level to produce images.

Inside the sample, assumed to be uncharged silicon, electrons were propagated in trajectory steps each of which was terminated by a scattering, boundary crossing, or trajectory termination event. The scattering events included elastic electron-nuclear scattering, inelastic secondary electron generation, and phonon scattering. Elastic scattering was modeled using the Mott cross-sections in NIST SRD 64.[13] Secondary electron generation was modeling using scattering tables computed using dielectric function theory without the single-pole approximation.[14] The phonon scattering model is based on that of Llacer and Garwin.[15] At the Si/vacuum interface, electrons reflected or refracted at the boundary according to a quantum mechanical barrier transmission model in which the potential energy was described by $U(x) = \Delta U / [1 + \exp(-2x / w)]$ with x the distance from the boundary, w = 1 nm, and ΔU = 3.75 eV. Secondary electrons were simulated in the same way as primary electrons. Simulation of an electron stopped when it either escaped the sample and was detected or when its energy dropped so low that escape was impossible. More details of JMONSEL's models were previously published.[3] Some of the resulting images are shown in Fig. 5.

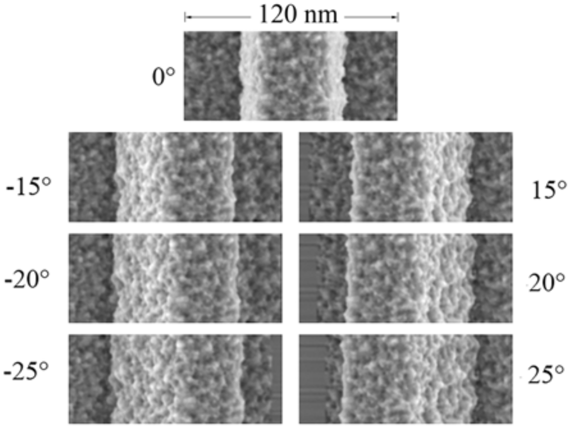


FIG. 5. Simulated 120 nm × 50 nm images of the virtual sample at several tilt angles.

3. 3D STEREO RECONSTRUCTION RESULTS

We purchased three commercial software packages, which we designate A, B, and C, with which to perform stereo reconstruction from our images. All packages provided an option to generate a text file containing (x,z) pairs on the surface of the reconstructed sample along a desired slice at constant y. We used this to generate the center profile from each reconstructed data set. A typical such result is shown in Fig. 6. This one was reconstructed from input images at –15º, –10º, and –5º. If the software accepted only two images, the middle image was omitted. In this case, reconstruction has a chance for accuracy for the visible parts of the sample on the top, left wall, and part of the substrate, but no chance to accurately reconstruct the right sidewall, which is hidden at these tilt angles. Thus, all the reconstructed profiles exhibit a characteristic and expected departure from the true profile on the right side. On the top and left side, packages A and B generally followed the trend though not the detailed roughness of the true profile. Package C generally follows the top and the left part of the substrate, but does a poorer job on the sidewall than A or B.

The immediate goal was a survey of quantitative errors in the height, width, and roughness of the line. A single image set centered on the usual top-view position, e.g., at 0º and ±5º, would be a poor choice for our purpose because each sidewall would be visible in only one of the 3 images. In order to have enough information to determine a width, it is necessary to reconstruct both the left and right sides of the line. This necessitated two sets of stereo images, one set all at negative tilts to make the left side visible in all its images, and another set all at positive tilts to make the right side visible. The negative set consisted of the three images at –25º, –20º, and –15º in Fig. 5. The positive set were the three at 15º, 20º, and 25º. None of the packages would accept more than one set at a time, so we performed separate reconstructions and stitched the results ourselves.

In order to obtain a height, both the top of the line and some part of the substrate must be reconstructed. Unfortunately, package C employed a windowing function that reconstructed a subset of the image smaller than the part visible in all images of the set. Because of this, this condition was not met. For this reason the remainder of the comparisons are restricted to the packages A and B. 3D visualizations of the left sidewall from these two are shown in Fig. 7.

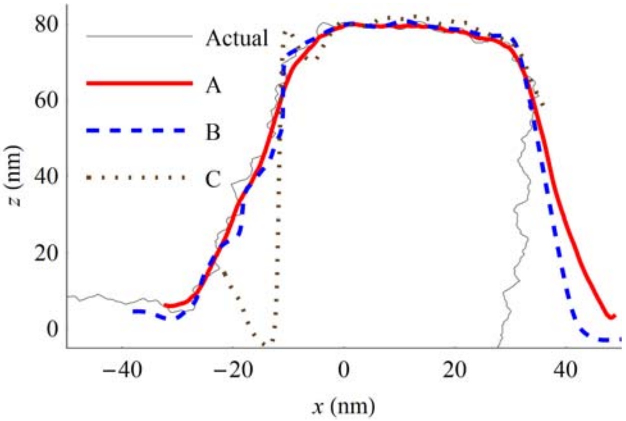


FIG. 6. Comparison of the actual sample surface profile and the reconstructed profiles from software packages A, B, and C.

To reconstruct full profiles, we stitched results obtained from opposite tilts by using the offsets that produced the best match for the top of the line, which was visible in both sets. For both A and B, there was some sensitivity of the determined lateral shift to the exact placement of the boundaries of "the top," e.g., whether the region stopped short of the rounded corners or extended into them. For a reasonable range of choices, the sensitivity (1 standard deviation) of the lateral shift was about 0.3 nm for A and 1 nm for B. The sensitivity of the vertical shift was much smaller, less than 0.1 nm for both A and B. With these offsets determined, the stitched profile was computed as a weighted average of the left and right profiles, with the weights a function of position. The left profile was weighted 100% for positions to the left of the top's left boundary, 0% for points to the right of the right boundary, transitioning linearly in between. The right profile weights were the reverse. The results are shown in Fig. 8, where they are compared to the true surface profile at that location.

For the purpose of quantifying differences between the reconstructed profiles and the true profile, we defined some relevant parts of each profile. Points in the profile were assigned to the left baseline by first selecting those that were left of the line center and with $z < z_0 + 0.05r$, where z_0 is the mean height of the leftmost 3 points and $r = z_{\mathrm{max}} - z_{\mathrm{min}}$ is the vertical range (the difference between the maximum and minimum z values in the profile). Then, of those points, the rightmost 3 nm were removed. Points were assigned to the left edge if their x coordinate was left of the line's center and their z coordinate satisfied $z_{\mathrm{min}} + 0.2r < z < z_{\mathrm{min}} + 0.8r$. The right baseline and right edge were defined by the mirror image of these procedures. Points were assigned to the top first by selecting those with $z_{\mathrm{max}} - 0.1h < z \le z_{\mathrm{max}}$ and then removing those within the first and last 5 nm. The clipping by several nanometers of the parts of the top and baseline nearest the sidewalls served to remove points associated with the transition between these regions.

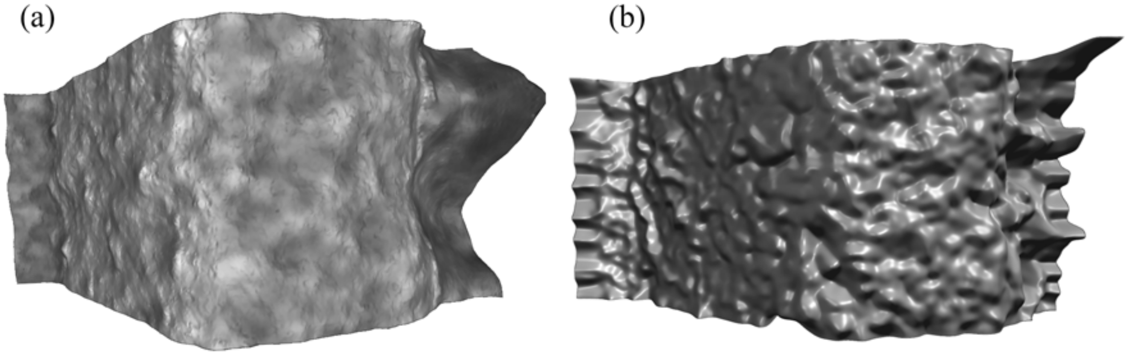


FIG. 7. 3D renderings of the left side provided by packages (a) A and (b) B.

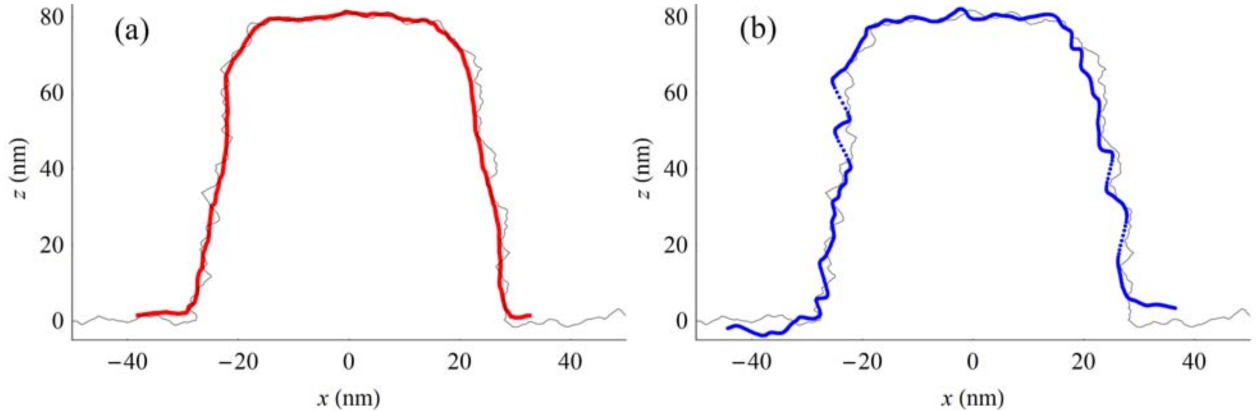


FIG. 8. Stitched reconstructions (thick lines) for software packages (a) A and (b) B compared to the true profile (thin line).

With these collections of points defined, the width was defined as $w = x_{\text{right}} - x_{\text{left}}$ with x_{right} and x_{left} the average of the x coordinates of points in the right and left sidewalls. Similarly, the height of the left edge was $z_{\text{top}} - z_{\text{leftBaseline}}$ the difference between the mean z coordinate of those points in the top and those in the left baseline. A height on the right was likewise defined. The standard deviation of z coordinates in the top region was designated σ_{top}. Since the sidewalls are nearly vertical, the sidewall roughness, $\sigma_{\text{sidewalls}}$, was computed as the standard deviation of the x coordinates after subtraction of a linear best fit trend line. The results of these operations are shown in Table 1. The rough skin that we wrapped around our line causes the true values of width and height for individual profiles to differ randomly from the whole-line mean values of 50 nm and 80 nm respectively. The tabulated true values are for our chosen profile, so they reflect this difference. The uncertainties attributed to the A and B widths reflect the stitching sensitivity to choice of boundaries for the area we matched.

4. DISCUSSION AND CONCLUSIONS

For height measurements, Package A had errors of –1.6 nm on the left and –0.7 nm on the right. Package B had errors of +2.3 nm on the left and –3.6 nm on the right. The average of Package B’s heights was 0.5 nm closer, but the average hides greater variability, which can be seen by visually comparing the left- and right-side heights in Fig. 8a and Fig. 8b. For width measurements, the errors were –0.9 nm and –0.6 nm for A and B respectively. Once again however, Package B had a higher variability, in this case because of the sensitivity of its result to the somewhat subjective designation of the “top” of the line. (Significant sensitivities are indicated by ±1 standard deviation values in Table 1.) A reason for the differences in these sensitivities is visible in Fig. 8. Package A’s profile has variation from the mean height that appear to more closely approximate those of the true profile (albeit somewhat too smoothly) than the variations in Package B’s profile. These variations play a strong role in determining the stitching of left and right profiles, which in turn is directly related to the determined width. Good consistency in these rough features between the left and right profiles leads to a strong correlation at a particular lateral offset. These observations about the rough top of the line carry over to the sides. In Fig. 8a, Package A’s profile appears to be a smoothed version of the actual profile. With that observation, it is not then surprising

TABLE 1. Comparison of actual and reconstructed heights and widths.

	True	**Package A**	**Errors A (result–true)**	**Package B**	**Errors B (result–true)**
h_{left} (nm)	79.5	77.9	–1.6	81.8	2.3
h_{right} (nm)	79.4	78.7	–0.7	75.8	–3.6
w (nm)	49.6	48.7 ± 0.3	–0.9 ± 0.3	49 ± 1	–0.6 ± 1
σ_{top} (nm)	1.8	1.3	–0.5	1.5	–0.3
$\sigma_{\text{sidewalls}}$ (nm)	0.9	0.4	–0.5	1.0	0.1

that the quantitative roughness determination in Table 1 shows this package's roughness values to be systematically low. Package B's are also somewhat low, though closer to those of the true profile. However, in Package B's profile in Fig. 8b, some of the roughness seems poorly correlated with the true profile. With its default filtering settings, this software's reconstruction had significant outliers. We specified increased filtering in order to perform the present reconstruction. It may be that some residue of these outliers remains in the form of roughness that is not correlated to actual roughness of the true profile. Package C had an unexpected limitation in the subset of the image set that it reconstructs. This limitation prevented us from including it in the detailed comparison that we have so far summarized. Had our line features occupied a smaller fraction of our simulated images we might have been able to do so. However, the partial (left side only) reconstruction in Fig. 6 suggests its errors would be larger than those of the other two packages.

SEM photogrammetry is subject to errors from many sources, not all of which are tested by the procedure described above. For example, in a real measurement we generally do not know exactly the sample tilt angles for the images that are used. The sample may vibrate, drift, or charge during imaging. The instrument's scale calibration may have errors, and its scan may not be perfectly linear nor the *x* and *y* axes exactly orthogonal. The sensitivity of 3D stereo reconstruction to these and other error sources were the subject of earlier work.[5-8]

However, there are other possible errors that are usefully and uniquely addressed through the use of virtual samples. Since the three software packages we tried above produced different reconstructions from the same input data set, it is evident that they are not using identical algorithms. Once homologous points within the image set are identified and located, the mathematics of reconstruction is well-established. Variability could be cause by faulty implementation in some of them. However, differences are not necessarily caused by errors. All three of the tested software packages use a preliminary pattern recognition step to identify homologous points within the image set. Typically such algorithms look for offsets in *x* and *y* that maximize the correlation between regions in the image set. A good correlation identifies corresponding regions in the images. However, correlation will not be perfect, partly because of noise in the images but also partly because the interaction of electrons with the sample is such that differences in appearance of a feature at different angles are not entirely explained by geometrical projection formulas. Algorithms may employ different strategies, approximations, amounts of filtering for noise reduction, etc., to strike different speed/accuracy trade-offs. Test problems with known correct answers are useful for algorithm testing, development, and validation. Since a virtual sample is a model in a computer, its true dimensions are known with mathematical accuracy, a level not achievable in real samples since these can only be known by virtue of a measurement that will have its own uncertainty, an uncertainty generally significant at the nanometer scale of interest to us.

Considered as a small survey of the available stereo reconstruction software, the fact that there were significant variations in the performance of different software packages suggests that the use of virtual samples has good potential to evaluate and then support and validate improvements in software quality. If there is a market for 3D reconstruction, and if differences in software quality are rendered easily visible by tests such as those described here, it seems likely that competition will drive more software closer to optimization. The fact that the best software had errors in width and height at only the ~1 nm level suggests that stereo reconstruction has good potential to support the electronics industry's need for better height information. To realize that potential it will be important to minimize errors from sources for which we did not test, such as errors in the tilt angles. SEMs would also need the ability to accurately mechanically tilt the sample or perform an equivalent electronic tilt of the beam's angle and scan direction.

REFERENCES

[1] B. Bunday, T.A. Germer, V. Vartanian, A. Cordes, A. Cepler, and C. Settens, "Gaps Analysis for CD Metrology Beyond the 22 nm node," *Proc. SPIE* **8681** (2013) 86813B.

[2] J. S. Villarrubia, A. E. Vladár, and M. T. Postek, "Scanning electron microscope dimensional metrology using a model-based library," *Surf. Interface Anal.* **37**, 951-958 (2005).

[3] J. S. Villarrubia, A. E. Vladár, B. Ming, R. J. Kline, D. F. Sunday, J. S. Chawla, and S. List, "Scanning electron microscope measurement of width and shape of 10 nm patterned lines using a JMONSEL-modeled library," *Ultramicroscopy* **154** (2015) 15-28, http://dx.doi.org/10.1016/j.ultramic.2015.01.004.

[4] G. Piazzesi, “Photogrammetry with the scanning electron microscope,” *J. Phys. E: Sci. Instrum.* **6** (1973) 392-397.

[5] P. Bariani, L. De Chiffre, H.N. Hansen, and A. Horsewell, “Investigation on the traceability of three dimensional scanning electron microscope measurements based on the stereo-pair technique,” *Prec. Eng.* **29** (2005) 219-228.

[6] F. Marinello, P. Bariani, E. Savio, A. Horsewell, and L. De Chiffre, “Critical factors in SEM 3D stereo microscopy,” *Meas. Sci. Technol.* **19** (2008) 065705.

[7] L. Carli, G. Genta, A. Cantatore, G. Barbato, L. De Chiffre and R. Levi, “Uncertainty evaluation for three-dimensional scanning electron microscope reconstructions based on the stereo-pair technique,” *Meas. Sci. Technol.* **22** (2011) 035103.

[8] T. Zhu, M.A. Sutton, N. Li, J.-J. Orteu, N. Cornille, X. Li, and A.P. Reynolds, “Quantitative Stereovision in a Scanning Electron Microscope,” *Exp. Mech.* **51** (2011) 97-109.

[9] C.A. Mack, “Generating random rough edges, surfaces, and volumes,” *Appl. Opt.* **52** (2013) 1472-1480.

[10] E.I. Thorsos, “The validity of the Kirchhoff approximation for rough surface scattering using a Gaussian roughness spectrum,” *J. Accoust. Soc. Am.* **83** (1988) 78-92.

[11] G. Palasantzas, “Roughness spectrum and surface width of self-affine fractal surfaces via the K-correlation model”, *Phys. Rev. B,* **48** (1993)14472–14478.

[12] Y. Zhao, G.-C. Wang, and T.-M. Lu, *Characterization of Amorphous and Crystalline Rough Surface: Principles and Applications,* Vol 37, Experimental Methods in the Physical Sciences (Academic Press, San Diego, CA) 2001 p. 38.

[13] A. Jablonski, F. Salvat, and C. J. Powell, NIST Electron Elastic-Scattering Cross-Section Database -Version 3.1, National Institute of Standards and Technology, Gaithersburg, MD (2002), http://www.nist.gov/srd/nist64.cfm

[14] S.F. Mao, Y.G. Li, R.G. Zeng and Z.J. Ding, “Electron inelastic scattering and secondary electron emission calculated without the single pole approximation,” *J. Appl. Phys.* **104**, 114907 (2008).

[15] J. Llacer and E.L. Garwin, “Electron-Phonon Interaction in Alkali Halides. I. The Transport of Secondary Electrons with Energies between 0.25 and 7.5 eV,” *J. Appl. Phys.* **40**, (1969) 2766.

A Sensor-Based Method for Diagnostics of Machine Tool Linear Axes

Gregory W. Vogl[1], Brian A. Weiss[1], and M. Alkan Donmez[1]

[1]*National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, 20899, USA*

gregory.vogl@nist.gov
brian.weiss@nist.gov
alkan.donmez@nist.gov

ABSTRACT

A linear axis is a vital subsystem of machine tools, which are vital systems within many manufacturing operations. When installed and operating within a manufacturing facility, a machine tool needs to stay in good condition for parts production. All machine tools degrade during operations, yet knowledge of that degradation is illusive; specifically, accurately detecting degradation of linear axes is a manual and time-consuming process. Thus, manufacturers need automated and efficient methods to diagnose the condition of their machine tool linear axes without disruptions to production. The Prognostics and Health Management for Smart Manufacturing Systems (PHM4SMS) project at the National Institute of Standards and Technology (NIST) developed a sensor-based method to quickly estimate the performance degradation of linear axes. The multi-sensor-based method uses data collected from a 'sensor box' to identify changes in linear and angular errors due to axis degradation; the sensor box contains inclinometers, accelerometers, and rate gyroscopes to capture this data. The sensors are expected to be cost effective with respect to savings in production losses and scrapped parts for a machine tool. Numerical simulations, based on sensor bandwidth and noise specifications, show that changes in straightness and angular errors could be known with acceptable test uncertainty ratios. If a sensor box resides on a machine tool and data is collected periodically, then the degradation of the linear axes can be determined and used for diagnostics and prognostics to help optimize maintenance, production schedules, and ultimately part quality.

1. INTRODUCTION

Linear axes are used to move components of machine tools that carry the cutting tool and workpiece to their desired positions for parts production (Altintas, Verl, Brecher, Uriarte & Pritschow, 2011). Essentially, a linear axis moves along a nominally linear path and is a vital subsystem of computer numerical control (CNC) machine tools. Because a typical 3-axis machine tool has three linear axes, their positional accuracies directly impact load capacity, quality, and efficiency of manufacturing processes.

As a machine tool is utilized for parts production, emerging faults lead to performance degradation, which lowers control precision and accuracy (Li, Wang, Lin & Shi, 2014). Typical faults within feed systems are due to pitting, wear, corrosion, cracks, and backlash (Zhou, Mei, Zhang, Jiang & Sun, 2009). As degradation increases, tool-to-workpiece errors become more likely, and eventually, linear axes of CNC machines may undergo significant wear that results in a failure and/or a loss of production quality (Uhlmann, Geisert & Hohwieler, 2008). Occurrences of faults and failures are becoming more common as higher levels of automation and productivity within manufacturing result in greater wear on machine components. Machine tool faults account for yearly economic losses of tens of billions of US dollars (Shi, Guo, Song & Yan, 2012). Thus, machine tools must be maintained and available for cost-effective production (Verl, Heisel, Walther & Maier, 2009).

Yet knowledge of degradation is illusive; accurately detecting degradation of linear axes is a manual, time-consuming, and potentially cost-prohibitive process. While direct methods for machine tool calibration are well-established (International Organization for Standardization, 2012) and reliable for position-dependent error quantification, measurements for these methods typically halt production and take "a long time" (Khan & Chen, 2009). The "extensive experimental and analytical efforts" for conventional sequential error measurement methods is usually time-consuming and requires expensive equipment, hindering widespread commercial adoption (Ouafi & Barka, 2013). Because degradation differs along a linear axis and the wear changes with production time (Uhlmann et al., 2008), the particular condition of an axis is usually unknown. The

Gregory Vogl et al. This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 United States License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Vogl, Gregory; Weiss, Brian; Donmez, M.
"A Sensor-Based Method for Diagnostics of Machine Tool Linear Axes."
Paper presented at the Annual Conference of the Prognostics and Health Management Society, Coronado, CA, Oct 18-Oct 24, 2015.

varying loads, hardness, and surface friction of guides affect their performance, so prediction of remaining useful life (RUL) of linear axis guideways may be difficult (Huang, Gao, Xu, Wu, Zhao & Guo, 2010).

Manufacturers need automated and efficient methods for continual diagnosis of the condition of machine tool linear axes without disruptions to production. This need is consistent with a European roadmap that identified three main key enabling technologies (KETs) for the future of sensor technology in manufacturing: new sensors and sensor systems, advanced sensor signal data processing, and intelligent sensor monitoring (Teti, Jemielniak, O'Donnell & Dornfeld, 2010). An online, condition monitoring system for linear axes is needed to help achieve the roadmap goals: decreased machine downtime, higher productivity, higher product quality, and enhanced knowledge about manufacturing processes (Teti et al., 2010).

Efforts to monitor the condition of linear axes components have utilized various sensors:

- Built-in linear and motor encoders (Plapper & Weck, 2001, Zhou, Tao, Mei, Jiang & Sun, 2011, Zhou, Xu, Liu & Zhang, 2014) with laser interferometer (Verl et al., 2009)
- Motor torque via current sensors (Li et al., 2014, Uhlmann et al., 2008, Zhou et al., 2009), accelerometers (Feng & Pan, 2012, Huang et al., 2010, Liao & Lee, 2009)
- Accelerometers, thermocouples, and analog controller outputs (torque, speed, and encoder position) (Liao & Pavel, 2012)
- Hall effect sensors (Garinei & Marsili, 2012)
- Piezoresistive thin films (Biehl, Staufenbiel, Recknagel, Denkena & Bertram, 2012, Möhring & Bertram, 2012)
- Piezoelectric ceramics (Ehrmann & Herder, 2013).

These attempts at condition monitoring of linear axes were limited in success, largely because both external sensors and built-in sensors have limitations. Built-in position sensors are usually highly accurate (Zhou et al., 2011), yet controller signals have problems such as low sample rate, limited sensitivity due to sensors being far from monitored components, and unwanted influences from multiple sources (Plapper & Weck, 2001). On the other hand, external sensors can be more direct and physically sensitive, but high costs and required bandwidths have impeded their application for online monitoring of linear axes (Zhou et al., 2009). Adding sensors to machine tools can also be very time-consuming with respect to setup, integration, and data communication.

In this paper, a new sensor-based method for diagnostics of machine tool linear axes is presented. The Prognostics and Health Management for Smart Manufacturing Systems (PHM4SMS) project at the National Institute of Standards and Technology (NIST) developed a sensor-based method to quickly estimate the performance degradation of linear axes. External sensors are used for high-bandwidth direct or indirect measurements of changes in linear axis errors. The sensors are contained within a 'sensor box' for ease of installation and periodic use on a machine tool for data collection and analysis, e.g., within 5 min. The diagnostics and prognostics of the linear axes can be used to help optimize maintenance, production schedules, and ultimately part quality. The cost-effective sensors are expected to be an overall net positive when factoring in the expected savings in production losses and scrapped parts for a machine tool.

2. SENSOR BOX CONCEPT FOR METROLOGY

The goal of the new sensor-based method is to enable efficient monitoring of the change in positioning errors, and hence the change in tool-to-workpiece positioning performance, due to degradation of linear axes. This section outlines these errors, the concept of the sensor-based methodology, and the needed uncertainties of the method.

2.1. Straightness and Angular Errors

Even without degradation, the carriage of a linear axis translates and rotates due to imperfections as the carriage moves along the guideways of the linear axis. Figure 1 shows these six errors that change with axis degradation. As the carriage is positioned along the X axis, it encounters three translational errors from its nominal path: one linear displacement error (E_{XX}) in the X-axis direction and two straightness errors (E_{YX} and E_{ZX}) in the Y- and Z-axis directions. The carriage also experiences three angular errors (E_{AX}, E_{BX}, and E_{CX}) about the X-, Y-, and Z-axes.

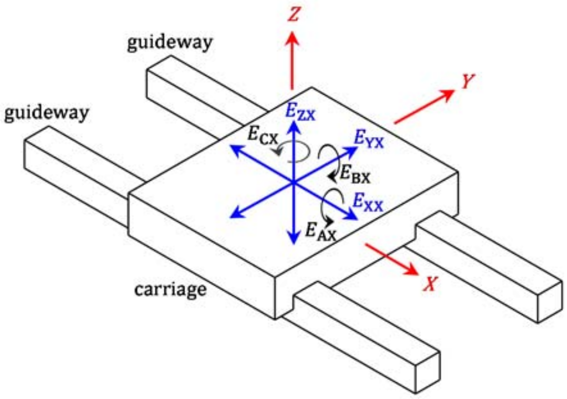


Figure 1. Translational and angular errors of a component commanded to move along a (nominal) straight-line trajectory parallel to the X-axis.

A typical machine tool has three linear axes, which means that a total of 18 (= 6 × 3) translational and angular errors exist. These errors are major contributors to the position-dependent tool-to-workpiece errors.

2.2. Sensor Box Concept

Sensors can be used to measure changes in the straightness and angular errors due to degradation. Figure 2 shows a sensor box on a typical 3-axis machine tool with 'stacked' linear axes; the Z axis is on the X axis, which is on the Y axis. The sensor box is attached to the Z-axis slide, so that if any axis is moved, the sensor box moves and will detect motion. Accelerometers are used to detect translational errors, and inclinometers and rate gyroscopes are used to detect angular errors. Some properties of these sensors are outlined in Table 1.

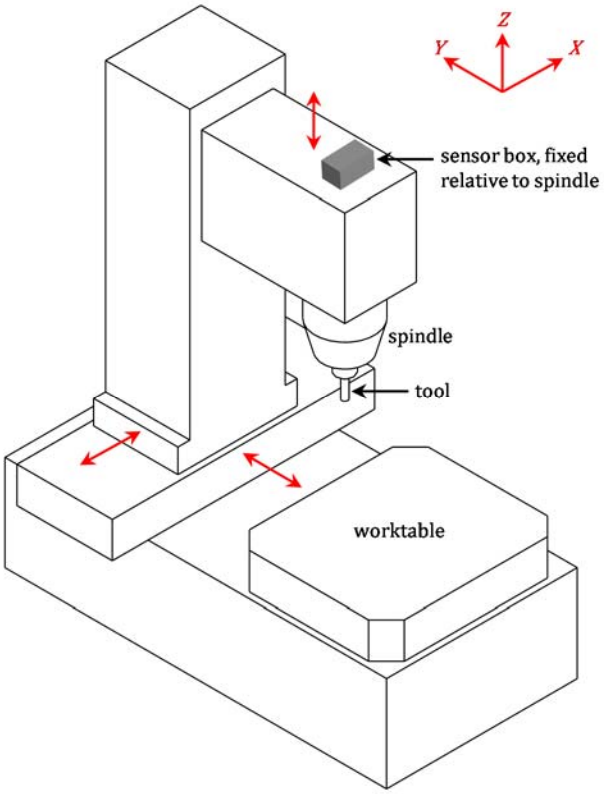


Figure 2. Schematic of sensor box on machine tool for metrology of linear axis degradation.

Table 1. Properties of sensors used in sensor box.

Sensor	Bandwidth[a]	Noise
Accelerometer	0.02 Hz to 1700 Hz	2.9 (μm/s^2)/√Hz at 1 Hz to 0.4 (μm/s^2)/√Hz at 1 kHz
Inclinometer	0 Hz to 2 Hz	2.4 μrad[b]
Rate gyroscope	0 Hz to 200 Hz	0.002 °/s/√Hz

[a] frequencies correspond to half-power points, also known as 3 dB points
[b] maximum deviation at 0 Hz

Once collected, the sensor data is processed to yield the straightness and angular errors. Specifically, rate gyroscope signals are integrated once to yield angular changes, and accelerometer signals are integrated twice to yield translational errors. Inclinometers may be used for direct measurement of angle from 0 Hz to about 2 Hz, as seen in Table 1. The reason for two types of angular sensors is that the inclinometer may measure low-frequency angular error terms with greater accuracy than the rate gyroscope.

Degradation may be tracked periodically by data collection during a fixed-cycle test (Garinei & Marsili, 2012, Huang et al., 2010, Liao & Lee, 2009, Verl et al., 2009, Zhou et al., 2009, Zhou et al., 2011). During a fixed-cycle test, the machine tool axes are commanded to move via the same program (the fixed cycle) with the machine tool initially in the same state (temperature, etc.) and undergoing the same nominal loads (cutting forces, if cutting occurs). The collected data is then processed, and the fixed-cycle results are compared to the previous results to determine the changes in straightness and angular errors. The deviations from one test to another are due to degradation, typically due to mechanical wear.

For the machine tool configuration highlighted in Figure 2, changes in the positioning errors could be estimated by using the data from the sensor box and the box's position relative to the tool tip. Therefore, the sensor box is focused on tracking the effects of degradation of each linear axis on the machining performance. For 4- or 5-axis machine tools with rotary axes, the rotary axes would be held fixed during motion of the linear axes. Also, for a different machine configuration without 3-axis stacking, an additional sensor box on the worktable would be necessary.

Details of the fixed-cycle test and data processing for the determination of error changes will be described in later sections.

2.3. Tolerances for Errors

The sensor-based method depends on the available sensors, whose selection depends on the magnitude of errors to be detected and the accuracy with which they need to be identified. Small levels of degradation of linear axes are expected and allowed, but there are limits specified for axis errors. ISO 10791-2 (International Organization for Standardization, 2001) specifies the tolerances for linear axis errors of vertical machining centers. As shown in Table 2, the acceptable straightness error is limited to 20 μm and the acceptable angular error is limited to 60 μrad.

Table 2. Tolerances for linear axis errors of vertical machining centers.

Error	Tolerance*
Straightness	20 μm
Angular (Pitch, Yaw, or Roll)	60 μrad

* for axes capable of 1 meter of travel, according to ISO 10791-2 (International Organization for Standardization, 2001)

The measurement uncertainties must be less than the respective specified tolerances to measure the errors. The test uncertainty ratio (TUR), which is the ratio of the tolerance to the uncertainty of the measurement, should be sufficiently large. Typically, a TUR of at least 4:1 is recommended; the larger, the better for a measurement system. For the measurement system to be created, we will accept a TUR of at least 4:1 based on design constraints such as sensor cost and size. Thus, we will accept straightness and angular error measurement uncertainties of 5 µm and 15 µrad, respectively, based on the tolerances outlined in Table 2.

3. SENSOR-BASED METHODOLOGY

A sensor-based method was developed to satisfy the TUR constraint of 4:1 and a total cost of about US$5000 for sensors. This section summarizes the sensor box, the fixed-cycle test, and the sensor-based methodology for determination of changes in straightness and angular errors.

3.1. Sensor Box

Figure 3 presents the sensor box, which is composed of two inclinometers, one tri-axial rate gyroscope (three rate gyroscopes), and three accelerometers. Each sensor detects a component of the translational or angular errors seen in Figure 1. The relationships of the sensors to these error components are noted in Figure 3.

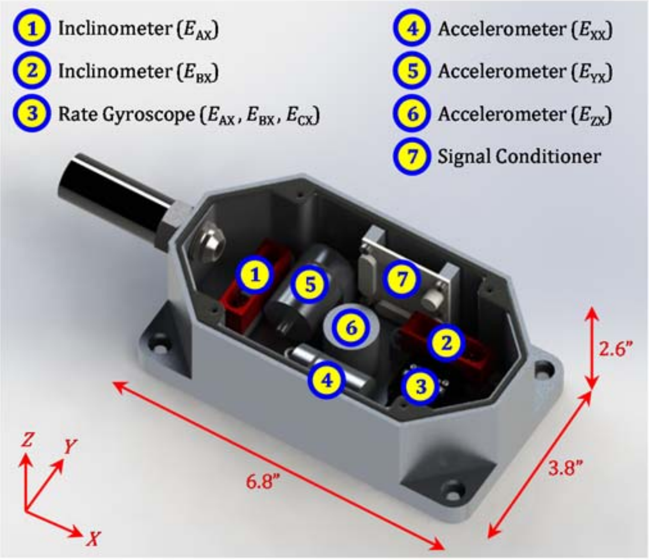

1 Inclinometer (E_{AX})
2 Inclinometer (E_{BX})
3 Rate Gyroscope (E_{AX}, E_{BX}, E_{CX})
4 Accelerometer (E_{XX})
5 Accelerometer (E_{YX})
6 Accelerometer (E_{ZX})
7 Signal Conditioner
2.6"
3.8"
6.8"
Z
Y
X

Figure 3. Rendered image of sensor box with sensors.

The sensor box top is not shown in Figure 3, so the sensors and their placement can be seen. When the sensor box top is attached, a rubber seal between the box top and base ensure that the sensors are sealed for protection from machine tool environments (including fluids, metal chips, etc.).

3.2. Fixed-Cycle Test

Table 3 summarizes the fixed-cycle test for degradation metrology. For the fixed-cycle test, each of the axes is operated sequentially to move over its entire travel range at three constant speeds typical of linear axes: 'Slow' axis speed = 0.02 m/s (50 s to travel 1 m), 'Moderate' axis speed = 0.1 m/s (10 s to travel 1 m), and 'Fast' axis speed = 0.5 m/s (2 s to travel 1 m). Different axis speeds are used to account for the various sensor bandwidths and noise properties seen in Table 1, in order to minimize the measurement uncertainties of the estimated translational and angular errors. For example, the inclinometer requires a 'slow' speed due to its bandwidth of 2 Hz, while the accelerometer requires faster speeds to sense low spatial frequency motions due to its low cutoff frequency of 0.02 Hz. If data is collected for only the forward motion of each axis of a 3-axis machine tool, then the data collection time totals about 3 min (= 3 × (50 s + 10 s + 2 s)).

Table 3. Fixed-cycle test for linear axis with a 1-m travel.

Sensor	Measurand
Axis Speed = 0.02 m/s	
Rate Gyroscope	Angular errors, 0.1 mm to 2 mm wavelength
Inclinometer	Angular errors, > 10 mm wavelength
Accelerometer	Straightness errors, 0.1 mm to 10 mm wavelength
Axis Speed = 0.1 m/s	
Rate Gyroscope	Angular errors, 2 mm to 10 mm wavelength
Accelerometer	Straightness errors, 10 mm to 100 mm wavelength
Axis Speed = 0.5 m/s	
Accelerometer	Straightness errors, 100 mm to 10 m wavelength

Sensor data is collected, integrated (as needed), filtered, and processed to yield the error components noted in Figure 3. These 'data fusion' processes are based on the fact that signals generated by the same geometric errors can be decomposed into various frequency components via filtering and then added together to yield the original errors. As seen in Figure 4, each filtered sensor signal yields a portion of the same geometric error over different neighboring spatial frequency ranges. Because these frequency ranges border each other, the error components add together to result in the originating geometric errors with wavelengths down to 0.1 mm.

Specifically, the rate gyroscope signal is filtered with 2-pole Butterworth filters, integrated, and then summed to the raw inclinometer signal to yield the angular errors. The only exception is for the Z axis, which does not have an inclinometer (as indicated in Figure 3), so the rate gyroscope is used alone to yield E_{CX}. Also, the filtered outputs from the accelerometer signals collected at different speeds can be summed, with the resultant acceleration integrated twice to yield straightness errors. The sensors must have relatively low noise in order to minimize drift, especially for the straightness errors based on double integration.

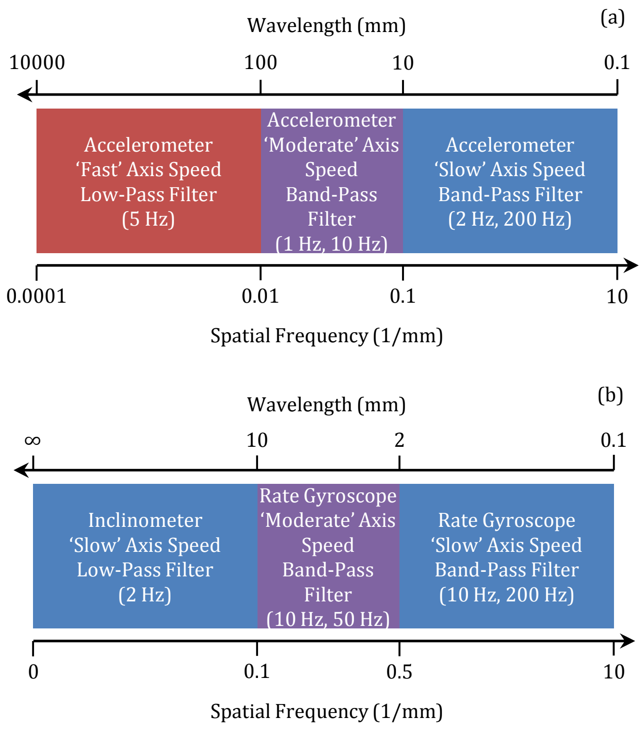


Figure 4. Fixed-cycle test data analysis for (a) straightness errors and (b) angular errors.

4. SENSOR-BASED METHOD UNCERTAINTY

Uncertainty is inherent with physical measurements, and the sensor-based method is no exception. Various sources of uncertainty exist, including sensor misalignment, calibration, and nonlinearity, as well as modal vibrations that could influence the signals. However, this section focuses on the expected main sources of uncertainty to the straightness and angular error estimates: sensor noise and the data fusion process described in Section 3.2.

4.1. Uncertainty Contributions from Sensor Noise

Each sensor has specified noise levels that influence the recorded sensor values. When processed according to Figure 4, sensor noise contributes uncertainty to the straightness and angular errors. Table 4 and Table 5 summarize these uncertainty contributions, determined from numerical simulations based on product specifications (e.g., see Table 1) in which 500 trials were used for statistical purposes. For example, the 10-second long (for the 'moderate' speed) simulated noise signal for the rate gyroscope was sampled at 25.6 kHz, a possible experimental sampling rate. The root mean square (RMS) of the spectral density of the white noise was scaled to match the RMS of the spectral density (0.002 °/√Hz) of the sensor, as specified in the product datasheet. The simulated noise was band-pass filtered with 2-pole Butterworth filters with a lower cutoff frequency of 10 Hz and an upper cutoff frequency of 50 Hz. Next, the filtered angular velocity was integrated to determine the angular displacement noise. Out of 500 trials, the mean was negligible, so the standard uncertainty is approximately the RMS deviation. The largest angular displacement was shown to be 6.2 μrad, and the RMS angular displacement was about 1.2 μrad for all trials, as seen in Table 5. Similarly, simulated acceleration signals were filtered and double-integrated to yield the translational displacement noises seen in Table 4.

Table 4. Straightness error uncertainties due to sensor noise.

Sensor	Axis Speed[a]	Filter	Expanded Uncertainty[b]	Standard Uncertainty
Accelerometer	Slow	Band-pass (2 Hz, 200 Hz)	0.081 μm	0.015 μm
Accelerometer	Moderate	Band-pass (1 Hz, 10 Hz)	0.14 μm	0.029 μm
Accelerometer	Fast	Low-pass (5 Hz)	0.26 μm	0.055 μm

[a] 'Slow' speed = 0.02 m/s, 'Moderate' speed = 0.1 m/s, and 'Fast' speed = 0.5 m/s

[b] defines an interval estimated to have a level of confidence of 99.8 percent

Table 5. Angular error uncertainties due to sensor noise.

Sensor	Axis Speed[a]	Filter	Expanded Uncertainty[b]	Standard Uncertainty
Inclinometer	Slow	Low-pass (2 Hz)	2.4 μrad	1.4 μrad[c]
Rate gyroscope	Moderate	Band-pass (10 Hz, 50 Hz)	6.2 μrad	1.2 μrad
Rate gyroscope	Slow	Band-pass (10 Hz, 200 Hz)	7.3 μrad	1.3 μrad

[a] 'Slow' speed = 0.02 m/s, 'Moderate' speed = 0.1 m/s, and 'Fast' speed = 0.5 m/s

[b] defines an interval estimated to have a level of confidence of 99.8 percent

[c] based on an assumed uniform distribution (NIST/SEMATECH, 2014)

The combined standard uncertainty over the full spatial spectrum due to sensor noise is equal to the square root of the sum of individual standard uncertainties listed in Table 4 or Table 5. Therefore, the combined standard uncertainty of the straightness error is 0.064 μm (= $[(0.015\ \mu\text{m})^2 + (0.029\ \mu\text{m})^2 + (0.055\ \mu\text{m})^2]^{1/2}$) and the combined standard uncertainty of the angular error is 2.3 μrad (= $[(1.4\ \mu\text{rad})^2 + (1.2\ \mu\text{rad})^2 + (1.3\ \mu\text{rad})^2]^{1/2}$). The combined expanded uncertainties for a coverage factor of $k = 5$, similar to those in Table 4 and Table 5, are 0.32 μm and 11.3 μrad, respectively, for straightness and angular errors.

The uncertainty evaluations are based on Monte Carlo propagation of the contributions from the recognized sources of uncertainty. The resulting expanded uncertainties are the half-widths of coverage intervals that include 99.8 % of the Monte Carlo sample of values of the measurand. The corresponding coverage factor was obtained as the ratio between the expanded uncertainty and the standard uncertainty. The unusually large size of this factor ($k = 5$) is attributable to the fact that the probability distribution of the measurand is markedly non-Gaussian.

Based on the tolerances of 20 μm and 60 μrad in Table 2, the TUR for noise-related straightness error is about 63:1 (=

20 µm / 0.32 µm) and the TUR for noise-related angular error is about 5:1 (= 60 µrad / 11.3 µrad). Because the TURs related to sensor noise satisfy the given constraint of 4:1, the sensors are acceptable.

4.2. Uncertainties of Sensor-Based Method

However, uncertainties of the straightness and angular errors are due to not only sensor noise, but also due to the data fusion process described in Section 3.2. Thus, the complete processes outlined in Figure 4 (with sensor noise included) were simulated for different randomly-generated straightness errors and angular errors within the tolerances (20 µm and 60 µrad) seen in Table 2. For any trial, the errors are generated in a process similar to a random-walk. Once generated, the simulated straightness and angular errors are considered to be the 'reference' errors, i.e., the 'true' errors, which can be compared to the 'estimated' errors resulting from the processes described in Section 3.2.

Figure 5(a) shows the three individual components of straightness error for one simulation that are summed to yield the estimated straightness in Figure 5(b). The 'Fast' axis-speed component is composed of the lowest frequency terms, while the 'Slow' axis-speed component is composed of the highest frequency terms.

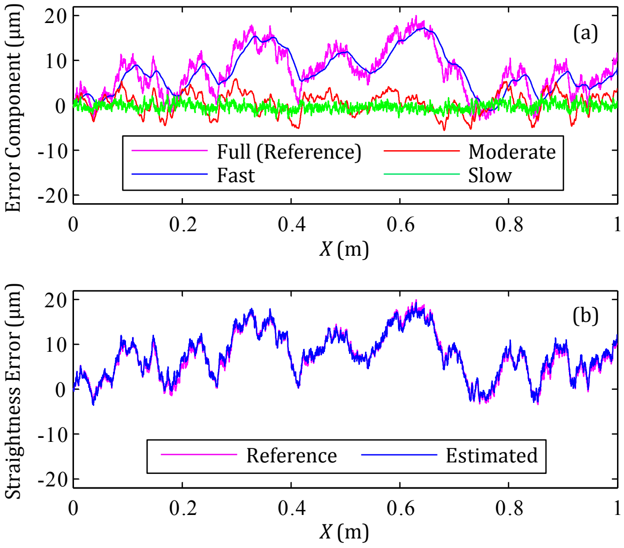


Figure 5. Example estimation of straightness error: (a) Straightness error component for each axis feed rate and (b) reference straightness error versus the estimated straightness error.

For 100 simulations with different randomly-generated straightness errors (the 'reference' errors), the difference between the reference and estimated straightness errors was within ± 5.6 µm, and the RMS of the difference over the entire axis travel was typically around 0.97 µm.

The estimation of the straightness and angular errors could be improved with averaging the results of multiple runs for data collection. For one case, Figure 6(a) shows the estimated angular error resulting from the use of 5 runs for averaging, and Figure 6(b) shows how the maximum and RMS values of *ΔError* (= estimated angular error – reference angular error) change with the number of runs used for averaging. Figure 6(b) shows that the maximum difference and RMS values approach 4.6 µrad and 1.4 µrad, respectively, as the number of runs for averaging increases. Both values do not approach zero as the number of runs increases towards infinity, because the process of Figure 4(b) is not perfect with respect to filtering or data fusion.

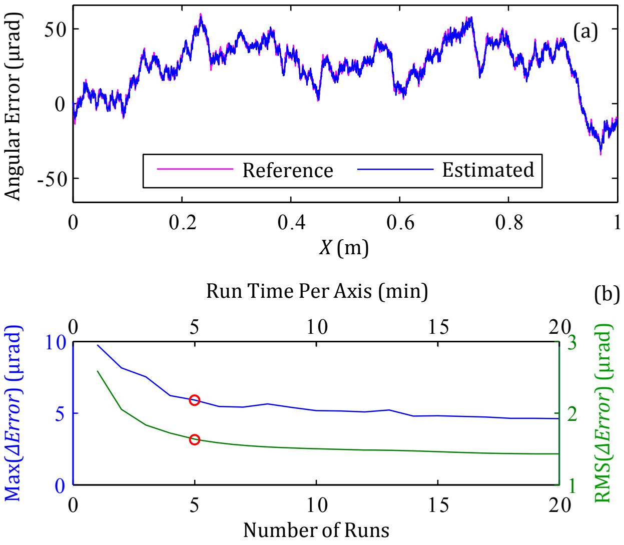


Figure 6. (a) the average estimated angular error for 5 runs and (b) the maximum and RMS values of *ΔError* versus the number of runs.

Table 6 shows the uncertainties of the sensor-based method for both straightness and angular error estimations with various numbers of runs for averaging (1, 5, or 10).

Table 6. Uncertainties of sensor-based method.

Error	Runs for Averaging	Expanded Uncertainty[a,b]	Standard Uncertainty[a]
Straightness	1	5.6 µm	0.97 µm
Straightness	5	4.1 µm	0.70 µm
Straightness	10	4.0 µm	0.65 µm
Angular	1	12.8 µrad	2.3 µrad
Angular	5	9.0 µrad	1.4 µrad
Angular	10	8.7 µrad	1.3 µrad

[a] for 100 simulations with different randomly-generated errors over a 1-m travel

[b] defines an interval estimated to have a level of confidence of 99 percent

Based on Figure 6(b) and Table 6, the number of runs should be no more than 5 runs (or 15 minutes of total data acquisition time for three axes), because more than 5 runs is time-consuming with minimal gain in accuracy. This result is consistent with, and helps to support, international machining standards that utilize 5 runs in any direction (positive or negative) for averaging purposes, e.g., Section A.3.1 in ISO 230-2:2014 (International Organization for Standardization, 2014).

4.3. Method Limitations

Based on Table 2 and Table 6, the TUR for straightness error is about 5:1 (= 20 µm / 4.1 µm) and the TUR for angular error is about 7:1 (= 60 µrad / 9.0 µrad) for 5 runs used for averaging. Both TURs satisfy the given constraint of 4:1, so the process described in Section 3.2 is acceptable.

Nonetheless, the method is limited because neither the sensors nor the data fusion process described in Section 3.2 are perfect. Comparison of the straightness error uncertainties due to either noise (see Table 4) or the entire method (see Table 6) shows that the latter is dominant; the accelerometer noise is a minor contributor to measurement uncertainty. In fact, the major source of straightness error uncertainty is the limited sensor bandwidth; the lower cutoff frequency of the accelerometer is not 0 Hz but rather 0.02 Hz (3 dB). Hence, the spatial frequency of Figure 4(a) does not reach down to 0 mm^{-1}. Figure 7(a) shows how the main local difference between the reference and estimated straightness errors is basically a low-frequency shift.

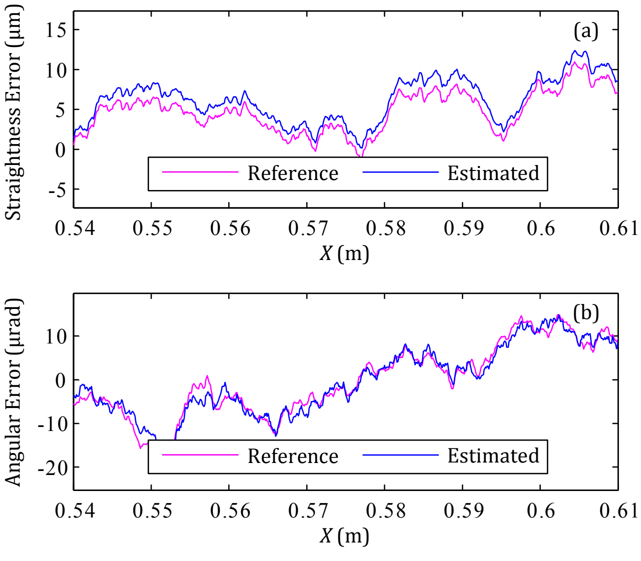


Figure 7. Typical section of (a) estimated straightness error and (b) estimated angular error, based on 5 runs used for averaging.

In contrast, Table 5 and Table 6 show how the angular sensor noise, especially that of the rate gyroscope, is a major contributor to the angular error uncertainty. Consequently, the main local difference between the reference and estimated angular errors is higher-frequency in nature, as seen in Figure 7(b).

5. IMPLEMENTATION OF SENSOR-BASED METHOD

The new sensor-based methodology for diagnostics of machine tool linear axes must be tested, validated, and verified experimentally. This section outlines the means for testing the accuracy of the sensor-based method for the detection of straightness and angular errors.

5.1. Linear Axis Testbed

A linear axis testbed was designed for testing the sensor-based method. As seen in Figure 8, the testbed is composed of a linear slide with a travel length of 300 mm. The linear slide is driven by a direct current (DC) motor with a rotary encoder attached to the motor shaft for motion control. Position is detected with a resolution of about 5 µm, which is much smaller than the 0.1 mm resolution of the method (see Table 3 or Figure 4) to enable repeatable test results.

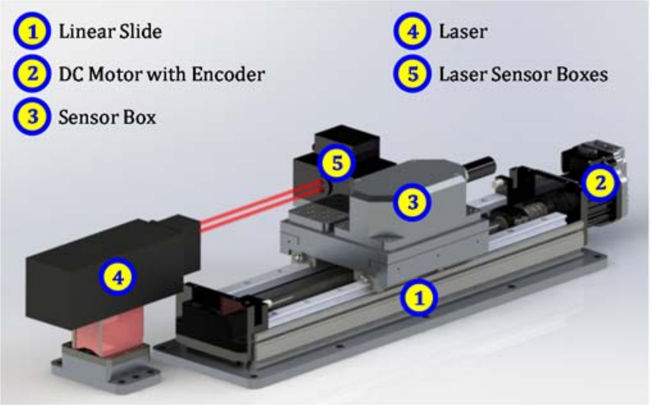


Figure 8. Rendered image of linear axis testbed for testing of sensor-based methodology.

Sensor boxes move with the carriage: the ‘sensor box’ for the new method and other boxes for a commercial laser-based system. The main laser sensor box contains optical technology to achieve a straightness error uncertainty of ±0.7 µm and an angular error uncertainty of ±3.0 µrad for 300 mm of travel. Due to its accuracy and precision, the laser-based system is used for validation and verification of the sensor-based method results.

5.2. Experimental Method

The sensor-based method must be tested to determine its efficacy in measuring changes, due to degradation, in straightness and angular errors of linear axes. One possible approach to induce degradation signals is to physically wear the linear slide, shown in Figure 8. However, such an approach is potentially time-consuming, expensive, and not repeatable due to unpredictable wear patterns.

In contrast, we choose to experimentally simulate degradation by replacing the default ball bearings with those of different diameters, as illustrated in Figure 9. The linear slide contains four 'blocks' or 'trucks', each with recirculating balls that contact the rails to constrain the carriage along its nominally linear path. Initially, every ball has the same nominal diameter of approximately 3.972 mm. These default balls can be replaced with balls of smaller or greater diameter to induce straightness and angular error changes of the carriage. The change (*ΔD*) of ball diameter is experimentally simple, quick, inexpensive, and repeatable.

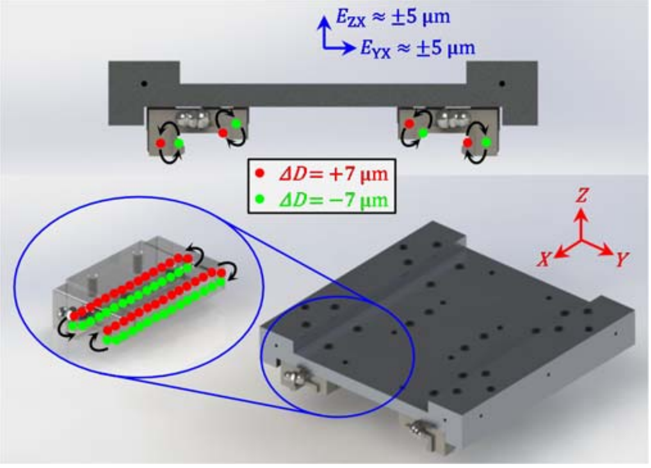


Figure 9. Example of experimental simulation of linear axis degradation via changes (*ΔD*) to ball diameters.

For example, Figure 9 shows how half of the balls can be replaced with balls that are 7 μm larger (*ΔD* = 7 μm) and the other half can be replaced with balls that are 7 μm smaller (*ΔD* = –7 μm). The net result is that the straightness errors, E_{YX} and E_{ZX}, will transition between about 5 μm and –5 μm as the carriage moves along the linear axis, for straightness error changes of about 10 μm. A variety of other ball configurations can cause translational or rotational changes of 20 μm or 60 μrad, respectively, which are the maximum acceptable errors according to Table 2. Therefore, patterns of balls of various diameters can be used to experimentally simulate error changes due to wear.

6. CONCLUSIONS

Manufacturers need quick and automated methods for continual diagnosis of machine tool linear axes without disruptions to production. Towards this end, a new sensor-based method was developed for linear axis diagnostics. The method uses a sensor box composed of inclinometers, accelerometers, and rate gyroscopes for high-bandwidth direct or indirect measurements of straightness and angular errors. When filtered and fused, the data yields seamless errors with wavelengths down to 0.1 mm. Simulations revealed that the multi-sensor-based method is capable of achieving test uncertainty ratios (TURs) of at least 4:1.

The sensor-based method must be validated and verified. Thus, a linear axis testbed was designed to allow testing of the new method against a commercial laser-based system. Various degradation patterns can be experimentally simulated by simple substitution of the bearing balls with balls of smaller or greater diameter.

Future tests will reveal the effectiveness of the new sensor-based method. Once the method is verified for diagnostics of linear axes, further tests may show the value of certain metrics for prognostic purposes to estimate the RUL. If the data collection and analysis are integrated within a machine controller, the process may seem to be seamless. Automated diagnostics and prognostics of linear axes can be used to help optimize maintenance and ultimately part quality. Therefore, the method is expected to generate a net positive with respect to decreased production losses for a machine tool.

ACKNOWLEDGEMENTS

The authors thank the Fabrication Technology (FT) Group (NIST) for their outstanding contributions with the experimental setup. This work was also served by invaluable discussions with Andreas Archenti (KTH Royal Institute of Technology, Sweden).

REFERENCES

Altintas, Y., Verl, A., Brecher, C., Uriarte, L., & Pritschow, G. (2011). Machine tool feed drives. *CIRP Annals - Manufacturing Technology,* vol. 60(2), pp. 779-796. doi: http://dx.doi.org/10.1016/j.cirp.2011.05.010

Biehl, S., Staufenbiel, S., Recknagel, S., Denkena, B., & Bertram, O. (2012). Thin film sensors for condition monitoring in ball screw drives. *1st Joint International Symposium on System-Integrated Intelligence 2012: New Challenges for Product and Production Engineering* (pp. 59-61), June 27-29, 2012, Hannover, Germany.

Ehrmann, C. & Herder, S. (2013). Integrated diagnostic and preload control for ball screw drives by means of self-sensing actuators. *2013 WGP Congress, July 22, 2013 - July 23, 2013* (pp. 271-277), Erlangen, Germany. doi: 10.4028/www.scientific.net/AMR.769.271

Feng, G.-H. & Pan, Y.-L. (2012). Investigation of ball screw preload variation based on dynamic modeling of a preload adjustable feed-drive system and spectrum analysis of ball-nuts sensed vibration signals. *International Journal of Machine Tools and Manufacture,* vol. 52(1), pp. 85-96. doi: http://dx.doi.org/10.1016/j.ijmachtools.2011.09.008

Garinei, A. & Marsili, R. (2012). A new diagnostic technique for ball screw actuators. *Measurement: Journal of the International Measurement Confederation,* vol. 45(5), pp. 819-828. doi: 10.1016/j.measurement.2012.02.023

Huang, B., Gao, H., Xu, M., Wu, X., Zhao, M., & Guo, L. (2010). Life prediction of CNC linear rolling guide based on DFNN performance degradation model. *2010 7th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2010* (pp. 1310-1314), August 10-12, 2010, Yantai, Shandong, China. doi: 10.1109/FSKD.2010.5569106

International Organization for Standardization (2001). *ISO 10791-2 - test conditions for machining centres − part 2: Geometric tests for machines with vertical spindle or universal heads with vertical primary rotary axis (vertical Z-axis).*

International Organization for Standardization (2012). *ISO 230-1 - test code for machine tools − part 1: Geometric accuracy of machines operating under no-load or quasi-static conditions*. Geneva, Switzerland: International Organization for Standardization (ISO).

International Organization for Standardization (2014). *ISO 230-2 - test code for machine tools − part 2: Determination of accuracy and repeatability of positioning of numerically controlled axes*.

Khan, A. W. & Chen, W. (2009). Calibration of CNC milling machine by direct method. *2008 International Conference on Optical Instruments and Technology: Optoelectronic Measurement Technology and Applications*, November 16-19, 2008, Beijing, China. doi: 10.1117/12.807066

Li, Y., Wang, X., Lin, J., & Shi, S. (2014). A wavelet bicoherence-based quadratic nonlinearity feature for translational axis condition monitoring. *Sensors,* vol. 14(2), pp. 2071-2088.

Liao, L. & Lee, J. (2009). A novel method for machine performance degradation assessment based on fixed cycle features test. *Journal of Sound and Vibration,* vol. 326(3–5), pp. 894-908. doi: http://dx.doi.org/10.1016/j.jsv.2009.05.005

Liao, L. & Pavel, R. (2012). Machine tool feed axis health monitoring using plug-and-prognose technology. *Proceedings of the 2012 conference of the society for machinery failure prevention technology*

Möhring, H.-C. & Bertram, O. (2012). Integrated autonomous monitoring of ball screw drives. *CIRP Annals - Manufacturing Technology,* vol. 61(1), pp. 355-358. doi: http://dx.doi.org/10.1016/j.cirp.2012.03.138

NIST/SEMATECH (2014). *E-handbook of statistical methods*: http://www.itl.nist.gov/div898/handbook/

Ouafi, A. E. & Barka, N. (2013). Accuracy enhancement of CNC multi-axis machine tools through an on-line error identification and compensation strategy. *2013 3rd International Conference on Advanced Measurement and Test, AMT 2013* (pp. 1388-1393), March 13-14, 2013, Xiamen, China. doi: 10.4028/www.scientific.net/AMR.718-720.1388

Plapper, V. & Weck, M. (2001). Sensorless machine tool condition monitoring based on open NCs. *2001 IEEE International Conference on Robotics and Automation* (pp. 3104-3108), May 21-26, 2001, Seoul, Korea, Republic of. doi: 10.1109/ROBOT.2001.933094

Shi, R., Guo, Z., Song, Z., & Yan, J. (2012). Resarch of mechanical components' performance degradation based on dynamic fuzzy neural network. *2012 International Conference on Computer Science and Service System, CSSS 2012* (pp. 1997-2000), August 11-13, 2012, Nanjing, China. doi: 10.1109/CSSS.2012.498

Teti, R., Jemielniak, K., O'Donnell, G., & Dornfeld, D. (2010). Advanced monitoring of machining operations. *CIRP Annals - Manufacturing Technology,* vol. 59(2), pp. 717-739. doi: http://dx.doi.org/10.1016/j.cirp.2010.05.010

Uhlmann, E., Geisert, C., & Hohwieler, E. (2008). Monitoring of slowly progressing deterioration of computer numerical control machine axes. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture,* vol. 222(10), pp. 1213-1219.

Verl, A., Heisel, U., Walther, M., & Maier, D. (2009). Sensorless automated condition monitoring for the control of the predictive maintenance of machine tools. *CIRP Annals - Manufacturing Technology,* vol. 58(1), pp. 375-378.

Zhou, Y., Mei, X., Zhang, Y., Jiang, G., & Sun, N. (2009). Current-based feed axis condition monitoring and fault diagnosis. *2009 4th IEEE Conference on Industrial Electronics and Applications, ICIEA 2009* (pp. 1191-1195), May 25-27, 2009, Xi'an, China. doi: 10.1109/ICIEA.2009.5138390

Zhou, Y., Tao, T., Mei, X., Jiang, G., & Sun, N. (2011). Feed-axis gearbox condition monitoring using built-in position sensors and eemd method. (pp. 785-793), Kidlington, Oxfordshire OX5 1GB, United Kingdom. doi: 10.1016/j.rcim.2010.12.001

Zhou, Y., Xu, H., Liu, J., & Zhang, Y. (2014). On-line backlash-based feed-axis wear condition monitoring technology. *11th IEEE International Conference on Mechatronics and Automation, IEEE ICMA 2014* (pp. 1434-1439), August 3-6, 2014, Tianjin, China. doi: 10.1109/ICMA.2014.6885910

BIOGRAPHIES

Dr. Gregory W. Vogl is a Mechanical Engineer at the National Institute of Standards and Technology (NIST) located in Gaithersburg, Maryland. He received his B.S. (2000), M.S. (2003), and Ph.D. (2006) degrees in Engineering Mechanics from Virginia Tech, Virginia, USA. Currently, Greg is a member of the *Prognostics and Health Management for Smart Manufacturing Systems* (PHM4SMS) project, which seeks to develop a methodology, protocols, and reference datasets to enable robust real-time diagnostics and prognostics for smart manufacturing systems. Previously, he designed, fabricated, and experimented on microelectromechanical systems as a National Research

Council Postdoctoral Researcher at NIST. He then joined the Production Systems Group, in which he worked on machine tool metrology and standards development. His interests include machine tool spindle health, diagnostic and prognostic methods, nonlinear dynamics, engineering mechanics, and metrology.

Dr. Brian A. Weiss has a B.S. in Mechanical Engineering (2000), Professional Masters in Engineering (2003), and Ph.D. in Mechanical Engineering (2012) from the University of Maryland, College Park, Maryland, USA. He is currently the Associate Program Manager of the *Smart Manufacturing Operations Planning and Control* program and the Project Leader of the *Prognostics and Health Management for Smart Manufacturing Systems* project within the Engineering Laboratory (EL) at the National Institute of Standards and Technology (NIST). Prior to his leadership roles in the SMOPAC program and the PHM4SMS project, he spent 15 years conducting performance assessments across numerous military and first response technologies including autonomous unmanned ground vehicles; tactical applications operating on Android devices; advanced soldier sensor technologies; free-form, two-way, speech-to-speech translation devices for tactical use; urban search and rescue robots; and bomb disposal robots. His efforts have earned him numerous awards including a Department of Commerce Gold Medal (2013), Silver Medal (2011), Bronze Medals (2004 & 2008), and the Jacob Rabinow Applied Research Award (2006).

Dr. Alkan Donmez is currently the Group Leader of the Production Systems Group as well as the Program Manager for the *Measurement Science for Additive Manufacturing* program in the NIST Engineering Laboratory. He has been with NIST for more than 25 years conducting and supervising research in advanced manufacturing sciences, including machine tool performance modeling and metrology, machining process metrology, as well as the recent efforts in metal-based additive manufacturing (AM). He has actively participated in national and international standard committees, developing machine tool performance testing standards, for more than 20 years. He has published more than 70 technical papers and reports in the area of machine tool metrology and manufacturing sciences. He has received various awards for his technical contributions, including R&D100, Applied Research Award of NIST, and Department of Commerce Silver and Bronze Medals.

Proceedings of the
Annual Stability Conference
Structural Stability Research Council
Orlando, Florida, April 12-15, 2016

New Component-Based Model for Single-Plate Shear Connections with Pre-tension

Jonathan M. Weigand[1]

Abstract
Although simple shear connections are typically idealized as perfectly pinned, the actual resistance of the gravity framing system to flexural and axial loads can be critical in evaluating the robustness and stability of steel buildings subjected to extreme loads such as earthquakes, fire, and column loss. There are several key reasons for including more realistic connection behaviors in the design and analysis of steel buildings for extreme loads: (i) the gravity connections may develop large localized deformations under combined flexural and axial loading, potentially precipitating their failure (e.g. due to local buckling, fracture of the bolts, etc.), (ii) the gravity connections provide critical lateral bracing to the columns, and failure of connections could lead to global instability (potentially resulting in disproportionate collapse), and (iii) accurately accounting for contributions from the gravity system in design could effectively reduce the demands on the lateral load-resisting system, thus reducing costs. In order to include contributions from the steel gravity frames in structural analysis and design, validated and computationally efficient analysis tools are needed. This paper describes a component-based model for single-plate shear connections that includes the effects of pre-tension and accommodates both standard and slotted holes, accounting for deformations associated with bolt slip, bolt bearing, and bolt shear. The model also accounts for load reversals and pinching effects associated with hysteresis, thus providing the capability to model the connections under arbitrary in-plane load histories. Validation cases show that the model is capable of simulating connection response under both earthquake and column removal loading.

1. Introduction

Tests of steel gravity framing systems have shown that steel gravity connections contribute to the capacity and robustness of structural systems subjected to extreme loads such as earthquakes, fire, and column removal. However, in the design of structures for seismic and/or wind loads, contributions from the gravity connections to the lateral-load resisting system are often ignored (with the gravity connections idealized as perfectly pinned), even though gravity connections may comprise the majority of the steel framing connections. Tests of bare-steel single-plate shear connections under earthquake loads have demonstrated that the connections provide moment capacities on the order of 15 % to 20 % of their beam plastic moment capacities, and when

[1] Research Structural Engineer, National Institute of Standards and Technology (NIST), Gaithersburg, MD, jonathan.weigand@nist.gov

composite with a concrete slab on steel deck, they provide capacities on the order of 30 % to 60 % of their beam plastic moment capacities (Liu and Astaneh-Asl 1999). Including contributions from the steel gravity frames in capacity calculations of the lateral force resisting system during the design stage could be advantageous in the design and analysis of new structures, by reducing the cost of the overall structural system and making steel moment frame or braced frame buildings more competitive with concrete buildings. Even if the gravity connections are not included in the design of the lateral load resisting system, including their contributions in building analyses under amplified design loads (i.e., the Federal Emergency Management Agency (FEMA) P-695 methodology (FEMA 2009)) could provide a quantifiable measure of inherent robustness (or reserve capacity) in the structural system, a topic of widespread current interest in the structural engineering community. A recent study on 1-, 2-, 4-, and 8-story non-ductile steel moment framed buildings subjected to the FEMA P-695 "Far-Field" ground motion set showed that including gravity frames in the building analyses reduced the probability of collapse by 45 % (on average), when compared with analyses of the moment frames only (Judd and Charney 2014).

The role of the gravity connections in the system robustness is potentially even more critical when considering the response of steel buildings to column loss. Large-scale tests of steel gravity framing systems under column removal (Johnson et al. 2014; Johnson and Meissner 2015) have shown that the system robustness is largely dependent on the capacity of the connections to remain intact after undergoing highly-localized rotation and axial displacement demands. However, the results of full-scale tests of steel gravity connections under column removal demands available in the literature remain limited to just a handful of connection configurations and load histories. To evaluate general structural robustness, researchers and engineers need accurate and validated analysis tools to simulate the connection behavior over a wide range of connection configurations and under more general load histories.

Several researchers (e.g., Sadek et al. (2008), Wen et al. (2013b), Main and Sadek (2014), Weigand (2014)) have shown that detailed finite element models can accurately simulate the behavior of single-plate shear connections under earthquake loads and/or column removal scenarios, which are used to evaluate the potential for disproportionate collapse. However, the need to model large structural systems in engineering design practice makes detailed modeling of complete structural systems infeasible. Main and Sadek (2014) recognized these limitations, and used results from their detailed finite element models to calibrate a biaxial spring to represent each bolt row in a single-plate shear connection, with stiffness parameters estimated based on linear regression of rotational stiffness data from seismic testing. They showed that a reduced-order modeling approach provided good agreement with push-down tests of two-span beam assemblies by Thompson (2009).

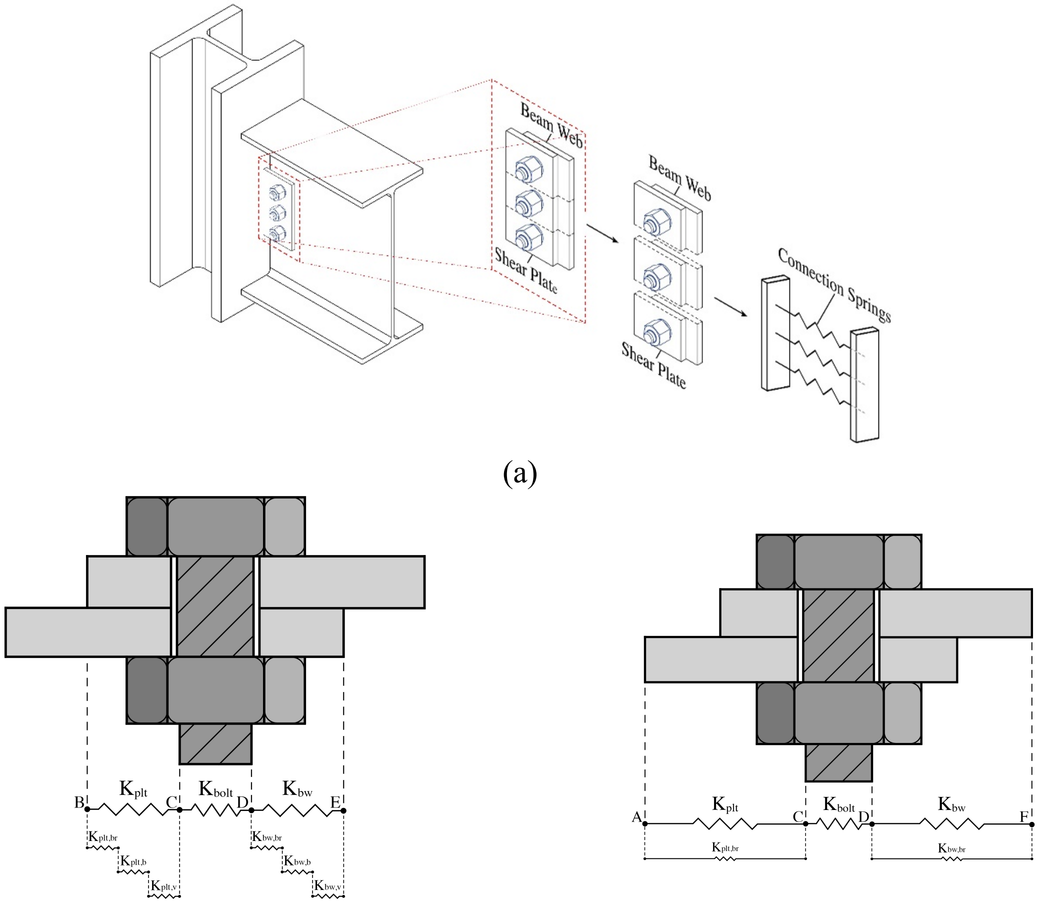
Other researchers (e.g., Liu and Astaneh-Asl (2004), Foley et al. (2006), Wen et al. (2013a)) have used lumped plasticity springs as a simplified means to capture the connection moment-rotation and axial force-deformation behaviors. While lumped plasticity models do provide a fairly complete description of the connection backbone response under pure rotation or pure axial deformation, they cannot account for interactions between the connection flexural and axial behaviors. Thus, they may not be appropriate for design under extreme loads as: (i) during earthquakes, the gravity connections may be subjected to significant axial loads in addition to rotations (Astaneh-Asl 2005), and (ii) for column removal scenarios, the development of catenary action requires the connections to accommodate large axial deformations in combination with large rotations (Sadek et al. (2008), Oosterhof and Driver (2012), Main and Sadek (2014), Weigand (2014)).

Component-based models provide a natural framework for capturing the complex behaviors of steel gravity connections under extreme loads as they including both fastener and connected element deformations, and provide automatic coupling between the in-plane flexural and axial behaviors. A number of component-based models are already available in the literature for certain types of steel gravity connections (e.g., bolted end-plate, bolted angle connections), but models for single-plate shear connections are relatively few. In addition to Main and Sadek (2014), described above, Elsati and Richard (1996) provided backbone response parameters for 76 mm (3.0 in) segments of single-plate shear connections and showed that component-based models could be used to model the connection pushover moment-rotation response. Weigand and Berman (2008) also used component-based models to determine the moment-rotation response of single-plate shear connections, but with the backbone response curve parameters taken from a model developed by Rex and Easterling (1996), and including multilinear hysteretic rules for the component unload/reload behaviors. Yu et al. (2009) likewise used the bolt-bearing curve developed by Rex and Easterling (1996) to model the backbone response of the connection segments, but with empirically modified stiffness values derived from finite element analysis results to model temperature dependence. Most recently, Koduru and Driver (2014) modified the empirical calibration factors determined by Yu et al. (2009), and also included shear yielding and shear fracture, to model the response of single-plate shear connections under column removal.

This paper summarizes a new component-based connection model for single-plate shear connections that includes the effects of pre-tension in the bolts and provides the capability to model connections with standard and slotted holes. The model is exercised under both cyclic rotations, representative of earthquakes, and combined rotations and axial deformations, representative of column removal scenarios. Results from these representative cases show that the model can be used to predict connection force and rotation/deformation capacities under both seismic loads and column removal scenarios.

2. Component-based Connection Model

In component-based connection models, the connection is notionally discretized into characteristic-width segments with aggregate force-displacement behaviors represented by discrete connection springs (Fig. 1a). Each characteristic-width segment captures contributions from the shear-plate, bolt, and beam-web, which are modeled as individual component springs in series as shown in Fig. 1(b) and Fig. 1(c)). The formulations for the backbone and hysteretic responses of the component springs are discussed in detail in the sections below.



(a)

(b)

(c)

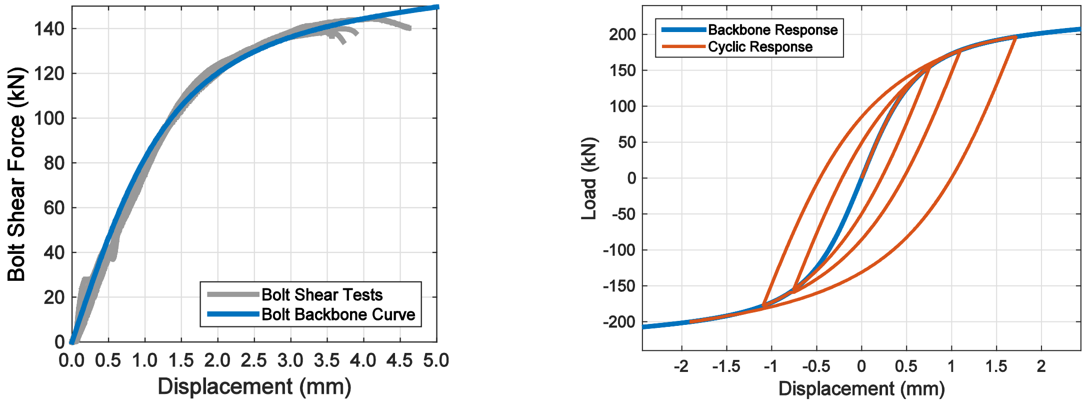
Figure 1: (a) Discretization of single-plate shear connection into connection springs, (b) connection spring stiffness contributions in tension, and (c) connection spring stiffness contributions in compression

2.1 Bolt Behavior

The transverse force-deformation behavior of the bolt, including shear and flexural effects, is modeled using Eq. (1) as:

$$R_{\text{bolt}} = R_{\text{unl}} + \frac{(K_{\text{i,bolt}} - K_{\text{p,bolt}})(\Delta_{\text{bolt}} - \Delta_{\text{unl}})}{\left(1 + \left|\frac{(K_{\text{i,bolt}} - K_{\text{p,bolt}})(\Delta_{\text{bolt}} - \Delta_{\text{unl}})}{R_{\text{cyc,bolt}}}\right|^{n_{\text{bolt}}}\right)^{\left(1/n_{\text{bolt}}\right)}} + K_{\text{p,bolt}}(\Delta_{\text{bolt}} - \Delta_{\text{unl}})\ , \qquad (1)$$

where Δ_{bolt} is the bolt shear deformation, R_{bolt} is the bolt shear force, $(\Delta_{\text{unl}}, R_{\text{unl}})$ are the coordinates of the last unload point, $R_{\text{cyc,bolt}} = \text{sign}(\Delta - \Delta_{\text{unl}})R_{\text{v,bolt}} - R_{\text{unl}} + K_{\text{p,bolt}}\,\Delta_{\text{unl}}$ is the cyclic reference load for the bolt shear force-deformation behavior where $R_{\text{v,bolt}} = 0.62F_{\text{u,bolt}}A_{\text{b}}$ (J3-1) is the shear capacity of the bolt, $n_{\text{bolt}} = 2$, A_{b} is the bolt cross-sectional area and $F_{\text{u,bolt}}$ is the tensile strength of the bolt material. Fig. 2(a) shows a comparison of the bolt backbone force-displacement response to data from three bolt-shear tests for 19 mm (3/4 in) diameter A325 bolts from Weigand (2014). Fig. 2(b) shows the behavior of the bolt under increasing magnitude cyclic shear deformations.



(a) (b)

Figure 2: (a) Comparison of bolt shear component spring backbone response with bolt shear data from Weigand (2014)[2], and (b) bolt shear component spring cyclic response

The initial stiffness of the bolt force-deformation response is calculated using the bolt bearing stiffness $K_{\mathrm{br,bolt}}$ and the bolt shearing stiffness $K_{\mathrm{v,bolt}}$ as

$$K_{\mathrm{i,bolt}} = \frac{1}{\frac{1}{K_{\mathrm{br,bolt}}}+\frac{1}{K_{\mathrm{v,bolt}}}} \quad . \tag{2}$$

The bearing stiffness is calculated as

$$K_{\mathrm{br,bolt}} = \frac{1}{1+3\beta_{\mathrm{b}}}\left(\frac{t_{\mathrm{p}}t_{\mathrm{w}}E_{\mathrm{bolt}}}{2t_{\mathrm{p}}t_{\mathrm{w}}}\right) \ , \tag{3}$$

based on the work by Nelson et al. (1983), where β_{b} is a correction factor that accounts for the concentration of bearing forces at the interface between plates for bolt in single shear. The value of β_{b} can range from 1 for a simple shear pin to relatively small values (on the order of 0.15) for pre-tensioned bolts with large bolt heads, washers, and nuts. For the analyses included in this paper, a value of $\beta_{\mathrm{b}} = 0.7$ was used. The bolt shearing stiffness is determined by assuming that the bolt acts as a prismatic Timoshenko beam with circular cross-section and fixed ends, such that:

$$K_{\mathrm{br,bolt}} = \frac{12E_{\mathrm{bolt}}I_{\mathrm{bolt}}}{L_{\mathrm{bolt}}^{3}(1+\Phi)} \ , \tag{4}$$

where E_{bolt} is the modulus of elasticity of the bolt, $I_{\mathrm{bolt}} = \pi d_b^2/64$ is the moment of inertia of the bolt shaft cross-section, $L_{\mathrm{bolt}} = t_{\mathrm{p}} + t_{\mathrm{w}}$ is the bolt length, and

$$\Phi = \frac{12E_{\mathrm{bolt}}I_{\mathrm{bolt}}}{L_{\mathrm{bolt}}^{2}\left(\frac{1}{\kappa G_{\mathrm{bolt}}A_{\mathrm{b}}}\right)} \tag{5}$$

[2] Estimated uncertainty in measured experimental data less than 1 %

is a term in Timoshenko beam theory that characterizes the relative importance of the shear deformations to the bending deformations (Thomas et al. 1973). In Eq. (5), $G_{\text{bolt}} = E/2(1+\upsilon)$ is the bolt shear modulus, and κ is the shear coefficient for a circular cross-section, defined as:

$$\kappa = \frac{1}{\frac{7}{6}+\frac{1}{6}\left(\frac{\nu}{1+\nu}\right)} \; . \tag{6}$$

The bolt plastic shear stiffness, $K_{\text{p,bolt}}$, was assumed to be 2 % of the bolt initial shear stiffness, $K_{\text{i,bolt}}$.

2.2 Shear Plate and Beam Web Behavior

The shear-plate and beam-web component springs (i.e., plate springs) are modeled using a piecewise version the Richard Equation (see Richard and Abbott (1975)) such that:

$$R(\Delta) = \begin{cases} \dfrac{(K_{\text{b}}^{-}-K_{\text{p}}^{-})(\Delta-\Delta_{\text{br}}^{-})}{\left(1+\left|\frac{(K_{\text{b}}^{-}-K_{\text{p}}^{-})(\Delta-\Delta_{\text{br}}^{-})}{R_{\text{b}}^{-}}\right|^{n_{\text{b}}^{-}}\right)^{\left(1/n_{\text{b}}^{-}\right)}} + K_{\text{p}}^{-}(\Delta-\Delta_{\text{br}}^{-}), & \Delta \leq \Delta_{\text{slipctr}} - \frac{1}{2}\Delta_{\text{slip}} \\ \dfrac{(K_{\text{i}}-K_{\text{y}})\Delta}{\left(1+\left|\frac{(K_{\text{i}}-K_{\text{y}})\Delta}{R_{\text{y}}}\right|^{n}\right)^{(1/n)}} + K_{\text{y}}\Delta, & \Delta_{\text{slipctr}} - \frac{1}{2}\Delta_{\text{slip}} \leq \Delta \leq \Delta_{\text{slipctr}} + \frac{1}{2}\Delta_{\text{slip}} \\ \dfrac{(K_{\text{b}}^{+}-K_{\text{p}}^{+})(\Delta-\Delta_{\text{br}}^{+})}{\left(1+\left|\frac{(K_{\text{b}}^{+}-K_{\text{p}}^{+})(\Delta-\Delta_{\text{br}}^{+})}{R_{\text{b}}^{+}(T)}\right|^{n_{\text{b}}^{+}}\right)^{\left(1/n_{\text{b}}^{+}\right)}} + K_{\text{p}}^{+}(\Delta-\Delta_{\text{br}}^{+}), & \Delta \geq \Delta_{\text{slipctr}} + \frac{1}{2}\Delta_{\text{slip}} \end{cases} \tag{7}$$

where the superscripts, $(\cdot)^{+}$ and $(\cdot)^{-}$, denote tensile and compressive deformations of the component spring, respectively, and the remaining parameters in Eq. (7) are defined below. Fig. 2(b) shows a schematic of the backbone response.

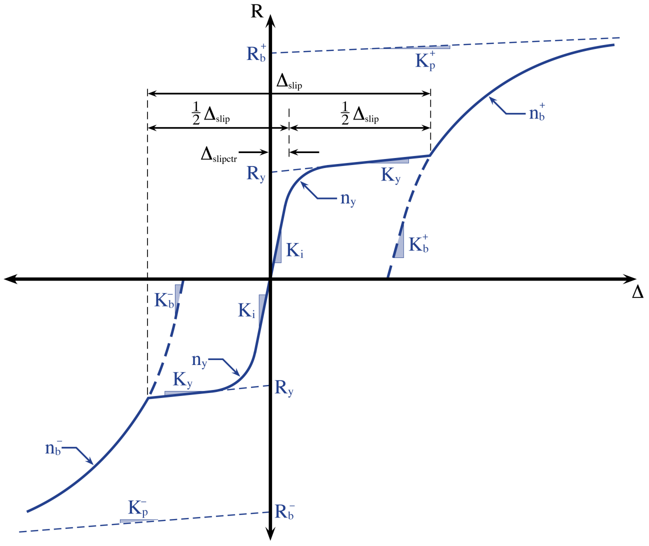


Figure 3: Plate component spring backbone force-displacement response

Prior to bearing, the single-plate shear connection resists load via friction due to the clamping force supplied by the bolt pre-tension and the surface contact between the bolt and plates. For slip-critical connections, the plates are assumed to behave elastically prior to slip, with initial stiffnesses determined from the gross areas of the plate characteristic-width segments as:

$$K_{\mathrm{i}} = \frac{wt_{\mathrm{p}}E}{a} \tag{8}$$

where w is the width of the shear plate segment, t_{p} is the plate thicknesses, E is the modulus of elasticity of the plate steel, and a is the distance between the column face to the bolt line. Connections that do not use pre-tensioned bolts may not develop the elastic plate stiffnesses, and thus may have significantly smaller initial stiffnesses. For connections without pre-tensioned bolts, the initial stiffness of the friction-slip behavior can be assumed to equal the initial plate bearing stiffness for the relevant loading direction, K_{b}^{+} or K_{b}^{-}, defined below.

Slip occurs as the loading overcomes the resistance supplied by the bolt pre-tension and friction between the sliding surfaces. After slip is initiated, the bolt continues to slip until the initiation of bearing contact between the bolt shaft and the bolt holes (at deformations of $\Delta_{\mathrm{slipctr}} - (1/2)\Delta_{\mathrm{slip}}$ in compression or $\Delta_{\mathrm{slipctr}} + (1/2)\Delta_{\mathrm{slip}}$ in tension, where Δ_{slip} is the difference between the plate hole diameter (or slot width, when applicable) and the bolt diameter).

The load at slip can be calculated as:

$$R_{\mathrm{slip}} = n_{\mathrm{f}}\mu\alpha A_b F_{\mathrm{u,bolt}} \;, \tag{9}$$

Where μ is coefficient of friction between the steel surfaces in contact, n_{f} is the number of faying surfaces (or slip planes), A_{b} and $F_{\mathrm{u,bolt}}$ were defined above, and α is the ratio of the bolt pre-tension load to the bolt tensile strength. For the modeling presented in this paper, $\alpha = 0.75$ was used and μ was taken as 0.338, corresponding to an average value calculated from a large set of data compiled by Grondin et al. (2007).

It should be noted that when connections are loaded dynamically, the load in the connection spring may decrease as the coefficient of friction decreases from the static to the kinetic coefficient of friction. However, most tests of single-plate shear connections, including those used for comparison with the model, have been conducted at sufficiently small loading rates that their behavior remained pseudo-static. For pre-tensioned bolts in pseudo-static tests, the resistance of the connection tends to remain relatively constant or even increase slightly as the bolts slip (e.g., Liu and Astaneh-Asl (2004), Weigand (2014)). While Eq. (7) allows for either positive or negative slip stiffnesses (designated as K_{y}), the comparison studies presented here found that a small positive value of 0.01 % of the initial stiffness was appropriate in all of the considered cases.

The capacity and stiffness parameters of bearing portion of the shear-plate and beam-web component behavior were adapted from the work of Rex and Easterling (1996), who performed 46 tests on a single bolt bearing against a single plate. The elastic and plastic bearing stiffnesses of the bearing force-deformation response can be determined from $K_{\mathrm{b}}^{+} = \beta_{\mathrm{s}}\overline{K}_{\mathrm{b}}\alpha_{K_{\mathrm{b}}}$ and $K_{\mathrm{p}}^{+} =$

$\beta_{\mathrm{s}}\overline{K}_{\mathrm{b}}\alpha_{K_{\mathrm{p}}}$, where $\beta_{\mathrm{s}} = 1$ for structural steel, $\alpha_{K_{\mathrm{b}}} = 1.731$, and $\alpha_{K_{\mathrm{p}}} = -0.009$ (see Rex and Easterling (1996)), and

$$\overline{K}_{\mathrm{b}} = \frac{1}{\frac{1}{\overline{K}_{\mathrm{b}}^{\mathrm{br}}}+\frac{1}{\overline{K}_{\mathrm{b}}^{\mathrm{b}}}+\frac{1}{\overline{K}_{\mathrm{b}}^{\mathrm{v}}}} \tag{10}$$

with elastic stiffness contributions resulting from direct bearing ($\overline{K}_{\mathrm{b}}^{\mathrm{br}} = 120t_{\mathrm{p}}F_{\mathrm{y}}d_{\mathrm{b}}^{\left(4/5\right)}$), bending ($\overline{K}_{\mathrm{b}}^{\mathrm{b}} = 32Et_{\mathrm{p}}\left(L_{\mathrm{ehp}} - d_{\mathrm{b}}/2\right)^{3}$), and shearing ($\overline{K}_{\mathrm{b}}^{\mathrm{v}} = (20/3)Gt_{\mathrm{p}}\left(L_{\mathrm{ehp}} - d_{\mathrm{b}}/2\right)$). In the equations for the stiffness contributions, t_{p} is the plate thickness, d_{b} is the bolt diameter, F_{y} is the yield strength of the plate material, E is the modulus of elasticity of the plate material, and G is the shear modulus of the plate material.

The bearing response of the plates in compression is more constrained than that in tension, due to the additional restraint against bending provided by the plate welds. The additional constraint leads to a marginally stiffer force-deformation response in compression, relative to that in tension, an effect has also been noted experimentally for single-plate shear connections under increasing magnitude reversed cyclic loading (Crocker and Chambers 2004). The component spring bearing force-deformation response in compression mirrors the response in tension, but with initial elastic and plastic bearing stiffnesses based only on the direct bearing stiffness such that $K_{\mathrm{b}}^{-} = \beta_{\mathrm{s}}\overline{K}_{\mathrm{b}}^{\mathrm{br}}\alpha_{K_{\mathrm{b}}}$ and $K_{\mathrm{p}}^{+} = \beta_{\mathrm{s}}\overline{K}_{\mathrm{b}}^{\mathrm{br}}\alpha_{K_{\mathrm{p}}}$. In compression, $\alpha_{K_{\mathrm{p}}} = 0.001$ is taken as a small positive value to avoid the potential for a negative tangent stiffness.

Load Reversal Behavior

The behavior of single-plate shear connections upon load reversal can be relatively complex, but adequately capturing those complexities is critical to modeling the load-history-dependent resistance and energy dissipation capacity of the connections. Tests on single-plate shear connections under seismic loads have shown that the connection moment-rotation response becomes increasingly pinched and nonlinear at large rotations (e.g., Crocker and Chambers (2004), Liu and Astaneh-Asl (2004)). At small rotations prior to bearing, friction supplied by pre-tensioned bolts resists sliding in both directions, and the cyclic friction slip behavior at load reversal can be characterized by

$$R = R_{\mathrm{unl}} + \frac{(K_{\mathrm{i}}-K_{\mathrm{y}})(\Delta-\Delta_{\mathrm{unl}})}{\left(1+\left|\frac{(K_{\mathrm{i}}-K_{\mathrm{y}})(\Delta-\Delta_{\mathrm{unl}})}{R_{\mathrm{cyc}}}\right|^{n_{\mathrm{y}}}\right)^{\left(1/n_{\mathrm{y}}\right)}} + K_{\mathrm{y}}(\Delta - \Delta_{\mathrm{unl}})\ , \tag{11}$$

where, similar to the bolt shearing response, $(\Delta_{\mathrm{unl}}, R_{\mathrm{unl}})$ are the coordinates of the last unload point and $R_{\mathrm{cyc}} = \mathrm{sign}(\Delta - \Delta_{\mathrm{unl}})R_{\mathrm{y}} - R_{\mathrm{unl}} + K_{\mathrm{y}}\,\Delta_{\mathrm{unl}}$ is the current value of the cyclic reference load. Eq. (11) represents a "full" (i.e., not pinched) cyclic hysteresis that is symmetric about the origin.

After bearing has been initiated, the plate component spring model also tracks the coordinates of the minimum and maximum unload points, $\left(\Delta_{\mathrm{unl,min}}, R_{\mathrm{unl,min}}\right)$ and $\left(\Delta_{\mathrm{unl,max}}, R_{\mathrm{unl,max}}\right)$ respectively. The load reversal behavior is then defined between the values of the minimum and maximum unload points within the current cycle, permitting the model to capture the evolution of the connection response with increased hole elongations due to bearing. Pinching in the connection begins at the initiation of bearing deformations as a result of the loss of pre-tension in the bolts. This phenomenon is captured within the shear-plate and beam-web component springs by allowing the pinching (the scalar parameter γ in Eq. (15) below) to vary as a function of accumulated bearing deformation. The pinched hysteresis response is formed from a combination of two response curves. The first curve is the general form of the Richard Equation, which represents the response with no pinching, written in terms of the bearing curve parameters:

$$R = R_{\mathrm{unl}} + \frac{(K_{\mathrm{b}}^{+} - K_{\mathrm{p}}^{+})(\Delta - \Delta_{\mathrm{unl}})}{\left(1 + \left|\frac{(K_{\mathrm{b}}^{+} - K_{\mathrm{p}}^{+})(\Delta - \Delta_{\mathrm{unl}})}{R_{\mathrm{cyc}}}\right|^{n_{\mathrm{b}}^{+}}\right)^{\left(1/n_{\mathrm{b}}^{+}\right)}} + K_{\mathrm{p}}^{+}(\Delta - \Delta_{\mathrm{unl}}) \ , \tag{12}$$

where $R_{\mathrm{cyc}} = R_{\mathrm{b}}^{+} + R_{\mathrm{y}}$ for the initial unload cycle, and $R_{\mathrm{cyc}} = R_{\mathrm{unl,max}} - R_{\mathrm{unl,min}}$ for all subsequent cycles. The second curve, which represents the fully pinched response, is defined using a Bézier curve (e.g., Farin (1993), Prautizsch et al. (2002)). The Bézier curve was chosen because it provides an adaptable smoothly transitioning approximation to a piecewise-linear curve, that can be defined to traverse a path through zero load at zero displacement with a small residual stiffness K_{res}, and to terminate at the appropriate minimum or maximum unload point, depending on loading direction. The Bézier curve is calculated as

$$\boldsymbol{B}(t) = \textstyle\sum_{i=0}^{n} B_i^n(t)\, \boldsymbol{P}_i \ , \tag{13}$$

where t is a parametric variable ranging from 0 to 1 (i.e., 0 at the current unload point and 1 at the current reload point),

$$B_i^n(t) = \binom{n}{i}(1-t)^{n-i} t^i \qquad i = 0, 1, \ldots, n \tag{14}$$

are Bernstein polynomials, $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ are the binomial coefficients, and $\boldsymbol{P}_i$ is the set of control points that define the curve trajectory (Fig. 4). Tests of connections under cyclic rotation cycles have shown that $K_{\mathrm{rel}}^{-} \approx (1/2)K_{\mathrm{b}}^{-}$ and $K_{\mathrm{rel}}^{+} \approx (1/2)K_{\mathrm{b}}^{+}$. At a given value of t, the Bézier curve resulting from Eq. (14) has two components, where the second component corresponds to the component spring load (i.e, $\boldsymbol{B}_2(t) = R_{\mathrm{BZ}}$). R_{BZ} represents load reversal behavior that is fully pinched.

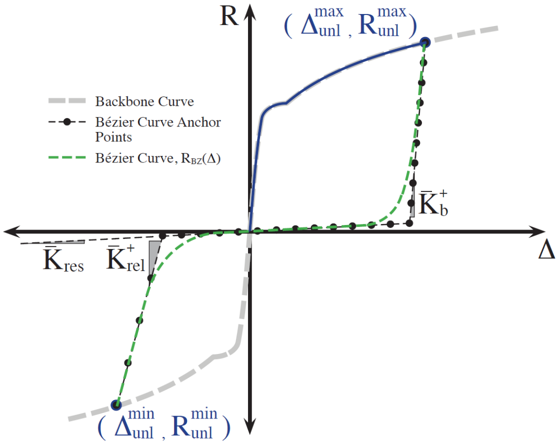

R
$(\Delta_{unl}^{max}, R_{unl}^{max})$
Backbone Curve
Bézier Curve Anchor Points
Bézier Curve, $R_{BZ}(\Delta)$
$\bar{K}_b^+$
$\bar{K}_{res}$
$\bar{K}_{rel}^+$
Δ
$(\Delta_{unl}^{min}, R_{unl}^{min})$

Figure 4: Schematic of Bézier curve with control points (unload from positive deformation)

The actual load reversal path R_p is calculated as a weighted summation between the full hysteretic behavior (i.e., Richard Equation) and fully pinched behavior (i.e., Bézier curve) as:

$$R_\text{p} = \gamma R + (1-\gamma) R_\text{BZ} \ , \tag{15}$$

where the amount that each curve contributes to the response defines the pinching ratio γ, which can vary between 0 and 1. Fig. 5(a) shows a schematic of the pinching behavior for the initial unload cycle and Fig. 5(b) shows a schematic of the pinching behavior for the subsequent cycles.

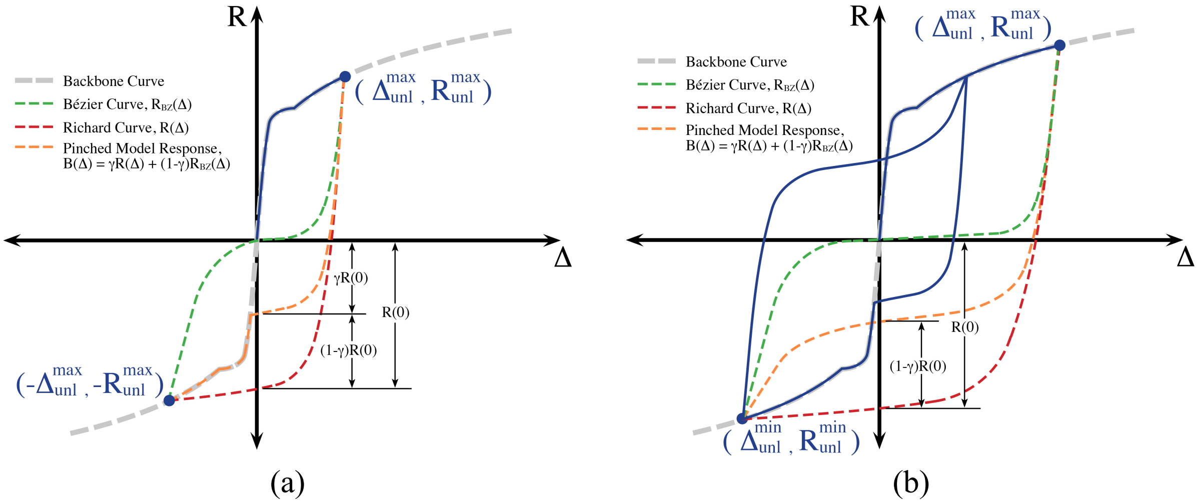
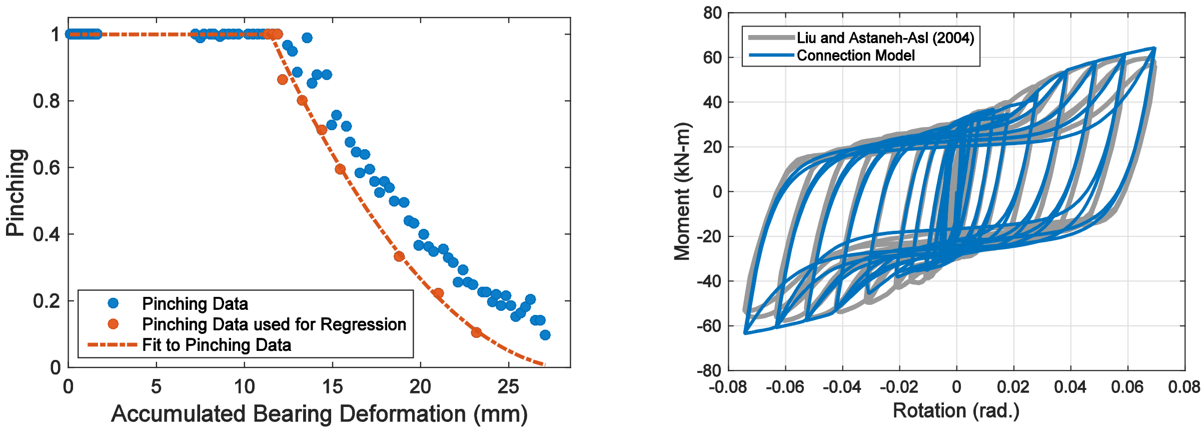

R
Backbone Curve
Bézier Curve, $R_{BZ}(\Delta)$
Richard Curve, $R(\Delta)$
Pinched Model Response, $B(\Delta) = \gamma R(\Delta) + (1-\gamma)R_{BZ}(\Delta)$
$(\Delta_{unl}^{max}, R_{unl}^{max})$
Δ
γR(0)
R(0)
(1-γ)R(0)
$(-\Delta_{unl}^{max}, -R_{unl}^{max})$
(a)
R
$(\Delta_{unl}^{max}, R_{unl}^{max})$
Backbone Curve
Bézier Curve, $R_{BZ}(\Delta)$
Richard Curve, $R(\Delta)$
Pinched Model Response, $B(\Delta) = \gamma R(\Delta) + (1-\gamma)R_{BZ}(\Delta)$
Δ
R(0)
(1-γ)R(0)
$(\Delta_{unl}^{min}, R_{unl}^{min})$
(b)

Figure 5: Schematic showing plate component spring pinched hysteresis (Eq. (15)) for (a) initial unload cycle and (b) subsequent unload cycle

Calibration of Pinched Hysteresis

The evolution of the pinching parameter γ was determined by assuming that the bolt behaves elastically, and calibrating the shear-plate and beam-web component-spring pinching behavior against data from Liu and Astaneh-Asl (2004), for a four-bolt single-plate shear connection subjected to increasing magnitude rotation cycles. The results of the pinching calibration are shown in Fig. 6(a), and Fig. 6(b) shows a comparison of the model response using the calibrated pinching function to the data from Liu and Astaneh-Asl (2004). More information on procedure used to calibrate the pinching parameter is available in Weigand (2016).



(a) (b)

Figure 6: (a) Pinching ratio data with fitted pinching curve, and (b) comparison of model response, using fitted pinching curve, to experimental data from Liu and Astaneh-Asl (2004)[3]

3. Calculation of Connection Deformations

The axial deformations of the connection springs, Δ_j, were calculated in terms of the connection rotation and axial deformation demands, θ and δ, respectively, using a rigid-body fiber-displacement model derived by Weigand and Berman (2014):

$$\Delta_\mathrm{j} = \delta + (1 - \cos\theta)X_{\mathrm{j}1} - \sin\theta X_{\mathrm{j}2} \quad , \tag{16}$$

where $\boldsymbol{X}_j$ denotes the location of the j^{th} connection spring with components $\boldsymbol{X}_j = \{X_{\mathrm{j}1}, X_{\mathrm{j}2}\}^T$ relative to the center of rotation of the connection (Fig. 7). For seismic tests, the connections are subjected only to rotation demands (i.e., $\delta = 0$), and the connection spring deformations are essentially linear with increasing rotation.

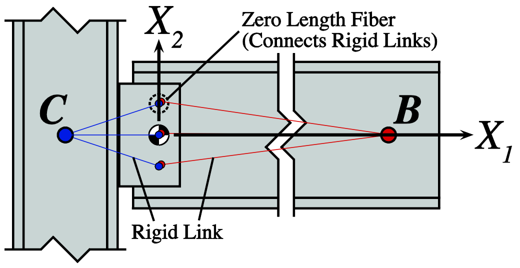


Figure 7: Coordinate system for calculation of spring displacements from rigid-body fiber displacement model (Source: Weigand and Berman (2014))

[3] Estimated uncertainty in measured experimental data less than 1 %

For the connections subjected to column loss, the connection demands can be calculated in terms of the vertical deflection of the simulated missing column, Δ_{syst}, (termed "simulated vertical displacement") as

$$\theta = \tan^{-1}\left(\frac{\Delta_{\mathrm{syst}}}{L_{\mathrm{r}}}\right) , \tag{17}$$

and

$$\delta = \frac{L_{\mathrm{r}}}{2}\left[\sqrt{1+\left(\frac{\Delta_{\mathrm{syst}}}{L_{\mathrm{r}}}\right)^2} - 1\right] , \tag{18}$$

where L_{r} is the distance between the centers of gravity of connection bolt groups on the ends of the framing members (in the undeformed configuration).

4. Results and Discussion

To examine the ability of the component-based model to adequately capture the connection response, the model was used to predict the responses of multiple tested connections for which data are available in the literature. Fig. 8 shows a comparison of the predicted response from the model to the moments at the peak rotations from each cycle of data from Crocker and Chambers (2000), for a 4-bolt single-plate shear connection with 19 mm (3/4 in) diameter A325 bolts, a 9.5 mm (3/8 in) thick A36 shear plate, and a W18×55 beam section. It should be noted that, because Crocker and Chambers (2000) listed the material grades used in the connection tests, but did not include coupon data for the shear plate and beam web materials, this comparison assumed plate material yield and ultimate tensile strengths equal to the expected material strengths from ANSI/AISC 341-10 (AISC 2005). Fig. 8 shows that the model underestimated the resistance of the connection at small rotations, relative to the connection data, but better approximated the peak moments of the connection at large rotations. During the cycle prior to connection failure in the test, the model was within 5 % of the moments at the peak rotations (4 % at the cycle peak and 1 % at the cycle valley).

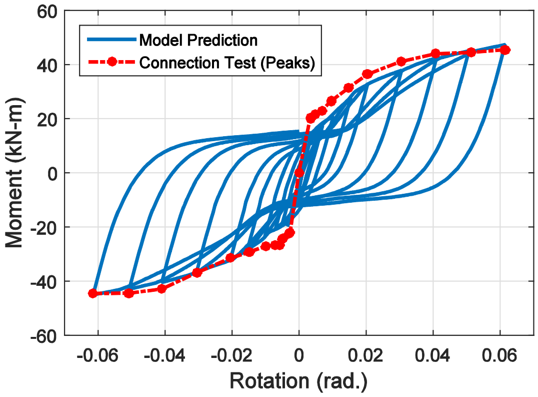
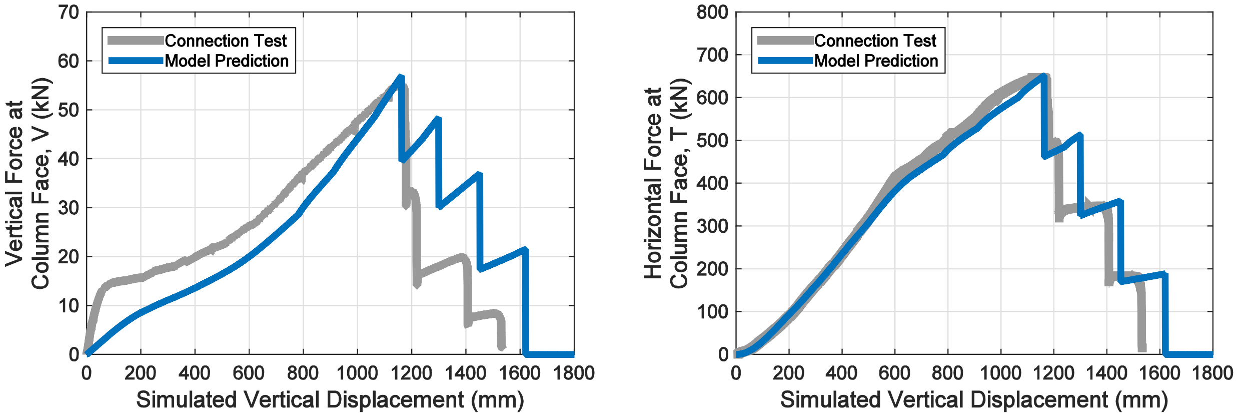


Figure 8: Comparison of moment-rotation response predicted by component-based model with connection data from Crocker and Chambers (2000)[4] (connection data shown at cycle peaks)

[4] Estimated uncertainty in measured experimental data less than 2 %

The component-based connection model was also compared to data from single-plate shear connection sub-assemblages tested by Weigand and Berman (2014) under simulated column removal. The model was subjected to the same rotation and axial deformation demands as were used in the sub-assemblage tests. The component spring displacements, due to the connection demands, were calculated from Eq. (16). Fig. 9 shows a comparison of the connection response predicted by the model with the vertical (i.e., along X_2) and horizontal (i.e., along X_1) force-displacement responses from Specimen sps4b|STD|34|38|48L from Weigand and Berman (2014), which corresponds to a 4-bolt single-plate shear connection with 19 mm (3/4 in) diameter bolts, a 9.5 mm (3/8 in) thick shear plate, and a 14.6 m (48 ft) span. The estimated uncertainty in the measured experimental data was less than ± 0.5 %, based on repeated calibrations of the instruments over the course of testing. The model under-predicts the connection vertical resistance throughout most of the analysis, relative to the connection data. This discrepancy occurs as a result of excess shear force in the tested connections, an effect which is described in detail in Weigand (2016). The model does not account for this excess shear force; however, as the excess shear force dissipates at large simulated vertical displacements (i.e., when the shear resistance of the connection is due primarily to tension resistance in the rotated configuration), the vertical force-displacement response of the model approaches that of the tested connection. The model predicted the peak vertical connection resistance within 4 % and the peak horizontal connection resistance within 1 %.



(a) (b)

Figure 9: Comparison of predicted (a) vertical force-displacement response and (b) horizontal force-displacement response from component-based model with connection data

5. Summary

This paper summarized the development of a component-based model for single-plate shear connections. The model was compared against the moment-rotation response of a single-plate shear connection tested under increasing magnitude rotation cycles (i.e., seismic loads), as well as against the vertical and horizontal force-displacement responses of a connections tested under combined rotation and axial deformation demands (i.e., column removal loads). The close agreement between the model and the connection experiments, as well as additional comparisons between the model predictions and connection test data presented in Weigand (2016), serve as validation of the proposed modeling approach.

Beyond predicting the responses of the single-plate shear connection tests considered in this paper for validation, the component-based model provides other key capabilities, such as the capacity to capture load reversals and energy dissipation, that are critical to modeling the responses of connections subjected to extreme loads. The model also accounts for the pinching effects associated with hysteresis, which are critical to modeling the history-dependent resistance of connections under seismic loads, and which also play a role in the behavior of connections subjected to column removal.

Acknowledgments

Valuable comments on this work were provided by Dr. Joseph A. Main of the National Institute of Standards and Technology.

Disclaimer

Certain commercial entities, equipment, products, or materials are identified in this document in order to describe a procedure or concept adequately. Such identification is not intended to imply recommendation, endorsement, or implication that the entities, products, materials, or equipment are necessarily the best available for the purpose. Official contribution of the National Institute of Standards and Technology; not subject to copyright in the United States.

References

AISC (2005). *Seismic Provisions for Structural Steel Buildings*. American Institute of Steel Construction, Inc.

Astaneh-Asl, A. (2005). "Design of Shear Tab Connections for Gravity and Seismic Loads." University of California at Berkeley, Berkeley, CA.

Crocker, J. and Chambers, J. (2004). "Single plate shear connection response to rotation demands imposed by frames undergoing cyclic lateral displacements." *Journal of Structural Engineering,* 130(6), 934-941.

Elsati, M.K. and Richard, R.M. (1996). "Derived Moment Rotation Curves for Partially Restrained Connections." *Structural Engineering Review,* 8, 151-158.

Farin, G. (1993). *Curves and surfaces for computer aided geometric design. A practical guide.* Academic Press.

FEMA (2009). *Quantification of Building Seismic Performance Factors*. FEMA P695, Prepared by the Applied Technology Council for the Federal Emergency Management Agency, Washington, D.C.

Grondin, G., Jin, M., and Josi, G. (2007). "Slip critical bolted connections – a reliability analysis for design at the ultimate limit state." *Report No. Structural Engineering Report 274,* University of Alberta, Edmonton, Alberta.

Johnson, E.S. Meissner, and Fahnestock, L.A. (2015). "Experimental Behavior of a Half-Scale Steel Concrete Composite Floor System Subjected to Column Removal Scenarios." *Journal of Structural Engineering,* 04015133.

Johnson, E.S., Weigand, J.M., Francisco, T., Fahnestock, L.A., Liu, J., and Berman, J.W. (2014). "Large-Scale Experimental Evaluation of the Structural Integrity of a Composite Steel and Concrete Building Floor System." *ASCE/SEI Structures Congress,* Boston, MA.

Judd, J.P. and Charney, F.A. (2014). "Seismic Collapse Prevention Systems." *Tenth U.S. National Conference on Earthquake Engineering,* Anchorage, AK.

Koduru, S.D. and Driver, R.G. (2014). "Generalized component-based model for shear tab connections." *Journal of Structural Engineering,* 04013041.

Liu, J. and Astaneh-Asl, A. (1999). "Cyclic Testing of Simple Connections Including Slab Effects." Volume I: Results of Test Series "A", *Report No. UCB/CEE-Steel-99-01,* University of California at Berkeley, Berkeley, CA.

Liu, J. and Astaneh-Asl, A. (2004). "Moment-rotation parameters for composite shear tab connections." *Journal of Structural Engineering,* 130(9), 1371-1380.

Main, J. A. and Sadek, F. (2012). "Robustness of Steel Gravity Framing Systems with Single-Plate Shear Connections". Report Number NIST.TN.1749, U.S. Department of Commerce, National Institute of Standards and Technology.

Oosterhof, S.A. and Driver, R.G. (2012). "Performance of Steel Shear Connections under Combined Moment, Shear, and Tension." *ASCE/SEI Structures Congress,* Chicago, IL, 146-157.

Prautizsch, H., and Boehm, W., and Paluszny, M. (2002). *Bézier and B-Spline Techniques*. Springer Science & Business Media.

Rex, C.O. and Easterling, W.S. (1996). "Behavior and modeling of a single plate bearing on a single bolt." *Report No. CE/VP-ST 96/14,* Virginia Polytechnic Institute and State University, Blacksburg, VA.

Richard, R.M. and Abbott, B.J. (1975). "Versatile elastic-plastic stress-strain formulation". *Journal of the Engineering Mechanics,* 101(EM4), 511-515.

Sadek, F., El-Tawil, S., and Lew, H.S. (2008). "Robustness of Composite Floor Systems with Shear Connections: Modeling, Simulation, and Evaluation". *Journal of Structural Engineering,* 134(11), 1717- 1725.

Thomas, D.L., Wilson, J.M., and Wilson, R.R. (1973). "Timoshenko beam finite elements." *Journal of Sound and Vibration*, 31(3) 315-330.

Thompson, S.L. (2009). "Axial, shear, and moment interaction of single plate "shear tab connections." Ph.D. Dissertation in Civil Engineering, Milwaukee School of Engineering, Milwaukee, WI.

Weigand, J.M. (2014). "The Integrity of Steel Gravity Framing System Connections Subjected to Column Removal Loading." Ph.D. Dissertation in Civil Engineering, University of Washington, Seattle, WA.

Weigand, J.M. and Berman, J.W. (2008). "Rotation and strength demands for simple connections to support large vertical deflections." 14th *World Conference on Earthquake Engineering*, Beijing, China.

Weigand, J.M. and Berman, J.W. (2014). "Integrity of Steel Single Plate Shear Connections Subjected to Simulated Column Removal." *Journal of Structural Engineering*, 145 (5).

Weigand, J.M. (2016). "A Component-based Model for Single-Plate Shear Connections with Pre-tension and Pinched Hysteresis." *Journal of Structural Engineering*. In review.

Wen, R., Akbas, B., and Shen, J. (2013a). "Practical moment-rotation relations of steel shear tab connections." *Journal of Constructional Steel Research*, 88, 296-308.

Wen, R., Akbas, B., Sutchiewcharn, N., and Shen, J. (2013b). "Inelastic behaviors of steel shear tab connections." *The Structural Design of Tall and Special Buildings*, 23, 929-946.

Yu, H., Burgess, I.W., Davison, J.B., and Plank, R.J. (2009). "Experimental investigation of the behavior of fin plate connections in fire." *Journal of Constructional Steel Research*, 65, 723-736.

Measurement Science for Prognostics and Health Management for Smart Manufacturing Systems: Key Findings from a Roadmapping Workshop

Brian A. Weiss[1], Gregory Vogl[2], Moneer Helu[3], Guixiu Qiao[4], Joan Pellegrino[5], Mauricio Justiniano[6], and Anand Raghunathan[7]

[1,2,3,4] *National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, 20899, USA*

brian.weiss@nist.gov
gregory.vogl@nist.gov
moneer.helu@nist.gov
guixiu.qiao@nist.gov

[5,6,7] *Energetics Incorporated, Columbia, Maryland, 21046, USA*

jpellegrino@energetics.com
mjustiniano@energetics.com
araghunathan@energetics.com

ABSTRACT

The National Institute of Standards and Technology (NIST) hosted the *Roadmapping Workshop – Measurement Science for Prognostics and Health Management for Smart Manufacturing Systems (PHM4SMS)* in Fall 2014 to discuss the needs and priorities of stakeholders in the PHM4SMS technology area. The workshop brought together over 70 members of the PHM community. The attendees included representatives from small, medium, and large manufacturers; technology developers and integrators; academic researchers; government organizations; trade associations; and standards bodies. The attendees discussed the current and anticipated measurement science challenges to advance PHM methods and techniques for smart manufacturing systems; the associated research and development needed to implement condition monitoring, diagnostic, and prognostic technologies within manufacturing environments; and the priorities to meet the needs of PHM in manufacturing.

This paper will summarize the key findings of this workshop, and present some of the critical measurement science challenges and corresponding roadmaps, i.e., suggested courses of action, to advance PHM for manufacturing. Milestones and targeted capabilities will be presented for each roadmap across three areas: *PHM Manufacturing Process Techniques*; *PHM Performance Assessment*; and *PHM Infrastructure – Hardware, Software, and Integration*. An analysis of these roadmaps and crosscutting themes seen across the breakout sessions is also discussed.

1. INTRODUCTION

The National Institute of Standards and Technology (NIST) is a research agency with the United States (U.S.) Department of Commerce that develops measurement science to advance innovative and emerging technologies to increase U.S. industry's competitiveness on a global scale. One specific area of NIST research is focused on Prognostics and Health Management for Smart Manufacturing Systems (PHM4SMS). To that end, it is critical for the NIST-PHM4SMS project team to understand the needs of its stakeholder community to develop and evolve the project's research plan, accordingly. A *Roadmapping Workshop – Measurement Science for Prognostics and Health Management for Smart Manufacturing Systems* was hosted by NIST on November 19th and 20th, 2014 to discuss the needs and priorities of stakeholders in the PHM4SMS technology area. The workshop brought together over 70 members of the PHM community including representatives from small, medium, and large manufacturers; technology developers and integrators; academic researchers; government organizations; trade associations; and standards bodies. The attendees discussed the current and anticipated measurement science challenges that they felt the PHM community should address to advance PHM methods and techniques for smart manufacturing systems. Attendees also described the

Brian A. Weiss et al. This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 United States License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

Weiss, Brian; Vogl, Gregory; Helu, Moneer; Qiao, Guixiu; Pellegrino, Joan; Justiniano, Mauricio; Raghunathan, Anand. SP-1064
"Measurement Science for Prognostics and Health Management for Smart Manufacturing Systems:
Key Findings From a Roadmapping Workshop." Paper presented at the Annual Conference of the Prognostics and Health Management Society, Coronado, CA, Oct 18-Oct 24, 2015.

associated research and development (R&D) needs that are hindering the advancement and implementation of condition monitoring, diagnostic, and prognostic technologies within manufacturing environments. Finally, attendees identified the priorities and next steps to meet the needs of PHM in manufacturing.

This paper begins by offering background on NIST's efforts in Smart Manufacturing and PHM in Section 2. Section 3 summarizes the key findings of the workshop including highlights from the panel discussions and breakout sessions. The breakouts focused the participants in three areas: *PHM Manufacturing Process Techniques*; *PHM Performance Assessment*; and *PHM Infrastructure – Hardware, Software, and Integration*. For each breakout, participants identified the area's goals, desired capabilities, challenges and barriers to developing these capabilities, and specific roadmaps with milestones and targets to achieve these goals and capabilities. Section 3 also highlights some of the crosscutting themes that emerged throughout the workshop. Section 4 concludes with a discussion of the NIST-PHM4SMS team's existing research plans.

2. BACKGROUND

2.1. Smart Manufacturing Systems (SMS)

NIST's mission is to promote U.S. competitiveness across many technological areas including manufacturing. Smart Manufacturing has been identified by numerous U.S. leadership organizations (including the Executive Office of the President) as a necessity for U.S. manufacturers to increase their global competitiveness (Manyika, Sinclair, Dobbs, Strube, Rassey, Mischke, Remes, Roxburgh, George, O'Halloran & Ramaswamy, 2012) (PCAST, 2012) (PCAST, 2014). Smart Manufacturing Systems (SMS) are the synthesis and integration of advanced physical and virtual technologies to enable innovative processes and enhance existing methods. SMS includes the convergence of information and communication technologies with a range of sophisticated and emerging capabilities in a wide range of domains including sensing, automation, machining, robotics, and additive manufacturing. The effective and efficient use, and integration of these technologies is promoting manufacturing growth by enabling manufacturers to increase their productivity, quality, and safety, while reducing their costs and waste (Bernaden, 2012).

NIST has developed a suite of Smart Manufacturing programs (including robotics and additive manufacturing) to address the measurement science challenges faced by manufacturers who are actively looking to grow and/or enhance their operations. One of the programs is the Smart Manufacturing Operations Planning and Control (SMOPAC) program which is designed to tackle technological and integration challenges posed at the factory level. PHM is a critical part of Smart Manufacturing. PHM may ultimately enable a machine or system to self-diagnose and self-heal with enough intelligence to be both aware of its current health and make an appropriate decision given both its state and goals. Presently, condition-monitoring, diagnostic, and prognostic techniques are not at the level required to enable this ultimate PHM vision; additional research is required.

2.2. Prognostics and Health Management for Smart Manufacturing Systems (PHM4SMS)

Within SMOPAC, the PHM4SMS project is aimed at developing the necessary measurement science to enable and enhance condition-monitoring, diagnostics, and prognostics. This measurement science includes the development of performance metrics, test methods, predictive modeling and simulation tools, reference data sets, protocols, and technical data.

The first of three phases of the PHM4SMS project is focused on assessment (the other phases are development and standardization): understanding the existing PHM capabilities, challenges, and needs of the manufacturing community and identifying the gaps that, if addressed, could benefit industry. This assessment phase has been marked by extensive research into PHM, both within literature reviews and direct interactions with PHM stakeholders (e.g., manufacturing process maintenance engineers, process design engineers, equipment operators). The NIST team has gained valuable insight about preventative/time-based maintenance (Ahmad & Kamaruddin, 2012) (Coats, Hassan, Goodman, Blechertas, Shin & Bayoumi, 2011); predictive maintenance/condition-based maintenance (Butcher, 2000) (Byington, Roemer, Kacprzymki & Galie, 2002) (Montgomery, Banjevic & Jardine, 2012) (Tian, Lin & Wu, 2012); and proactive/intelligent maintenance including maintenance at complex system levels (Barajas & Srinivasa, 2008) (Lee, Ghaffari & Elmeligy, 2011) (Lee, Ni, Djurdjanovic, Qiu & Liao, 2006).

Likewise, studies and reviews have been identified that compare existing PHM methods along with highlighting their strengths and limitations (Kothamasu, Huang & VerDuin, 2006) (Muller, Crespo Marquez & Iung, 2008) (Peng, Dong & Zuo, 2010). More specifically, reviews of PHM-based standards have also been conducted (Vogl, Weiss & Donmez, 2014a) (Vogl, Weiss & Donmez, 2014b) (Zhou, Bo & Wei, 2013).

Besides NIST efforts in reviewing the existing PHM techniques and standards landscapes, NIST has actively engaged numerous manufacturers to directly understand their PHM capabilities, successes, challenges, and needs. This has included site visits with many small, medium, and large manufacturers from a range of industries including automotive, aerospace, defense, earth-moving, and electro-mechanical. Stakeholder engagement peaked with the planning and execution of the *Roadmapping Workshop on Measurement Science for Prognostics and Health Management for Smart Manufacturing Systems*.

3. WORKSHOP

The NIST PHM4SMS project team contracted with workshop facilitation and documentation experts at Energetics Corporation to host a two-day workshop. This workshop brought together PHM stakeholders including small, medium, and large manufacturers; technology developers and integrators; standards bodies; academic researchers; and U.S. government organizations. This section summarizes the workshop activities and the output information from the participants. The full details can be found in the comprehensive workshop report (National Institute of Standards and Technology, 2015a).

3.1. Goals

The workshop was planned and executed with three specific goals. They were to identify and prioritize the:

- Measurement science needs for improving PHM impacts within manufacturing processes;
- Measurement science barriers, challenges, and gaps that prevent the broad use of PHM technologies for manufacturing processes;
- R&D needed to address the priority measurement and standards challenges.

3.2. Plenary Talks and Panel Discussions

The workshop featured five plenary talks and three panel discussions (National Institute of Standards and Technology, 2015b). The plenary talks, presented by NIST personnel and external PHM experts, talked about the needs to evolve PHM technology within manufacturing along with existing PHM successes that several organizations have recently employed. Likewise, the talks highlighted specific challenges that still remain that, if addressed, can present tremendous benefit to the manufacturing community. These challenges included the development of common standards, interoperability among systems, deriving actionable intelligence from extensive data streams, and enabling machines to self-heal (i.e., impending faults or failures and automatically take corrective actions to remedy the problem).

The three panel sessions are discussed in the following sub-sections. Each panel was moderated, and included numerous speakers from diverse industry backgrounds, each with practical PHM experience. Some of the highlights from the question and answer sessions during each panel will be discussed herein. Full presentations given by both the plenary speakers and panelists can be found on the NIST web space (National Institute of Standards and Technology, 2015b).

3.2.1. Panel 1: PHM Capabilities, Best Practices, Challenges, and Needs

This panel focused on the current state of PHM for manufacturing. Panelists focused on PHM technologies and systems including existing capabilities, best practices, and challenges along with technological gaps and limitations. Some of the key highlights of the panel's question and answer session include:

- Communication and interoperability at the system level – Diversity, varying ages, and non-standard software of numerous systems add complexity to PHM systems. Enhancing, simplifying, and standardizing communications among multiple systems is warranted to streamline PHM.
- Catalog of data sets for understanding failure – It is challenging to obtain sufficient training data to ascertain when equipment or processes will fail. It is rarely practical to let a machine or process fail solely to obtain a realistic data set. Given that the best data is often from real failures, data must be opportunistically captured when a true fault or failure occurs.
- Real-time aspects of PHM technologies – Manufacturers are seeing an increasing need for real-time PHM technologies. This is especially true for high value equipment or processes where any faults or failures can be detrimental to overall manufacturing operations. Not all organizations are ready for this shift; some are still lacking in basic (not real-time) PHM while others do not see the implementation of real-time PHM as being cost effective for their operations.

3.2.2. Panel 2: Performance Assessment – Monitoring and Measurement

This panel discussed the techniques for monitoring and measuring the performance of the PHM systems, themselves, along with identifying the metrics that evaluate how PHM technologies impact overall manufacturing performance. Highlights from this panel's question and answer session include:

- Equipment monitoring and data collection by suppliers – It is challenging to implement PHM in one's own organization and it can also be challenging to request PHM be integrated into an external supplier's operations. Those suppliers that integrate PHM within their operations will likely gain a competitive advantage in that they will have more forewarning of faults and/or be more capable of handling unforeseen failures.

- Cost justification of PHM systems – When manufacturers buy manufacturing equipment that has a history of reliable operations, it is unlikely that they will also want to invest in PHM for this same equipment. The cost justification can be made in terms of maintaining or increasing quality and/or safety. Manufacturers will gain confidence in their equipment if PHM technology providers support any warranties that are tied to the equipment.

3.2.3. Panel 3: PHM and the Human Element

The third panel focused on the influence and understanding of human decision-making on PHM systems within manufacturing and the difficulties that present themselves when humans work with PHM. A few of the highlights of this panel's question and answer session include:

- Need for increased knowledge of refurbished equipment – It is difficult to accurately assess a machine's health after it has been repaired (following a fault or failure), refurbished, or undergone extensive maintenance. This lack of knowledge can also complicate understanding a system's overall health when a constituent component has been extensively repaired or replaced. This situation presents an opportunity to develop inventory tracking in conjunction with PHM that could document individual health states and expected remaining useful life (RUL) of specific components.
- PHM is easier to implement at the onset of a machine's/process' life – It is more cost effective and easier to integrate PHM into equipment or a process during the design stage prior to the equipment or process being put into service. This ease of implementation includes making it easier to integrate sensors, technology, and programming for PHM. One disadvantage of integrating PHM at the onset is that it is likely that all of the faults and failures that could/will occur are not known at this initial timeframe; some faults and failures are still likely to occur that the PHM system would either not detect or inaccurately detect. PHM design and implementation is costly, so the specificity and extent of its capabilities should be measured against the projected savings with its usage.

3.3. Breakout Sessions

The workshop featured three separate breakout topics: *PHM Manufacturing Process Techniques and Metrics, PHM Performance Assessment*; and *PHM Infrastructure – Hardware, Software, and Integration*. Each breakout topic met four times (Sessions I, II, III, and IV) across the two-day event and held a specific focus:

- Breakout Session I: Goals and Desired Capabilities – For each topic area, the first session focused on capturing the specific PHM capabilities most wanted and needed. Each group identified goals in the near-term (1 to 2 years), mid-term (3 to 5 years), and long-term (5+ years) time horizons. Additionally, each group then categorized the capabilities in the different topic areas in terms of high, medium, and low priorities.
- Breakout Session II: Challenges and Barriers for Achieving the Capabilities – This breakout meeting for each topic focused on identifying the specific measurement and standards barriers, challenges, and gaps that hinder PHM development, implementation, and integration.
- Breakout Session III: Prioritization of Challenges – This breakout meeting identified R&D and standards priorities for each of the challenges and barriers mentioned in the prior session. This included organizing the challenges in terms of high, medium, and low priorities.
- Breakout Session IV: Pathways for a Measurement Science Roadmap – The final breakout meeting organized each topic's participants in small groups to develop specific roadmaps with recommended approaches, next steps, and actionable plans. Each action plan was also broken out into near-term (1 to 2 years), mid-term (3 to 5 years), and long-term (5+ years) timeframes.

Each of the three breakout topics will be presented in the following subsections. Although the three breakout groups operated separately, some of their identified goals, capabilities, challenges, and priority roadmaps had similar themes. This was natural in that some of these similarities cut across multiple topic areas. Cross-cutting themes are highlighted in Section 3.4.

In the following sections, highlights will be presented for all three breakout topics with a focus on the output roadmaps. Certain roadmaps were selected from each breakout topic for discussion in this paper. The chosen roadmaps were deemed the most important to address immediately and/or were supported by a majority of the participants while being relevant to NIST's mission.

3.3.1. Breakout Topic: *PHM Manufacturing Process Techniques and Metrics*

The successful implementation of PHM can have a significant influence on manufacturing operations by providing timely actionable intelligence. This intelligence can then be used to aid maintenance such that downtime is carefully coordinated with manufacturing operations for zero loss of productivity and quality. This breakout topic focused on addressing the specific PHM manufacturing process capabilities that can enable this timely actionable intelligence along with the metrics necessary to collect and analyze in support of these capabilities. This group focused on PHM techniques and metrics that can ultimately enhance condition-monitoring, equipment and process reliability, safety, operator situational awareness, and overall equipment effectiveness. After the group identified their desired goals and capabilities, and the corresponding challenges and barriers, three priority roadmap topics were developed. Two of the roadmaps are presented below while the third (Enterprise-Wide PHM for Maintenance Planning) is not discussed due to space restrictions.

Advanced Sensors for PHM in Smart Manufacturing

The development of this specific roadmap was spurred by the lack of understanding of the full suite of capabilities of sensors, their interfaces and interoperability needs for PHM. This is critical to address because current PHM systems lack re-configurability, flexibility, scalability, and robustness partly due to the lack of knowledge with respect to sensors.

A sub-group within this breakout session focused on outlining a multi-stage method for sensor development. This approach begins by inventorying existing sensor data acquisition (DAQ) systems that are needed for PHM systems and defining the re-configurability requirements for common manufacturing processes. This effort would ultimately breed data communications and analytics standards to promote greater communication among multiple configurations and technologies. Mid-term activities would include the identification of gaps in sensor and DAQ capability and interoperability, and define scalability requirements for several manufacturing processes. Long-term activities feature the development of multi-purpose sensors/DAQ interfaces for use within manufacturing PHM systems; development of standards for data communication, data analysis, and prognostic algorithms; and the development of a taxonomy of PHM systems and capabilities. This would lead to the generation of a taxonomy library and a PHM-handling catalog of generated tools to promote flexible and reconfigurable PHM systems. The completion of this roadmap action plan is envisioned to have high impact within the manufacturing community since it’s very likely to improve reliability/reduce failures of equipment and processes, improve maintenance scheduling, and speed process re-configurability.

PHM Data Format and Architecture

The generation of this roadmap was motivated by the desire to solve the lack of interoperability of sensors/data formats and types of communication while preserving the meaning of the data and the semantics. The overall approach of this roadmap is to create protocols for PHM covering formats, storage, organization, semantics, and other key components. Standards would be created to support the protocols along with data interfaces and integration. These protocols and overall architecture would enable the generation of a database of PHM data and information that the community could draw upon.

The near-term activities of this roadmap include determining protocol data types and structure. Guidelines must also be developed for data format, storage and preservation, organization, and semantic requirements. Moving forward, the mid-term activities would focus on standards development for semantic PHM data and the creation of tools to capture and organize the data; and then, extract and visualize the information in a meaningful way. The long-term tasking would focus on the creation, organization, and management of PHM data repositories. This would yield an expansive database that could be used by manufacturers, technology integrators, and technology developers who work with PHM systems. The advancement of this roadmap would have the highest impacts in speeding process re-configurability and improving maintenance scheduling.

3.3.2. Breakout Topic: *PHM Performance Assessment*

Before any new technology can realize its full potential, it is critical to verify and validate its performance. PHM is no exception, and care must be taken to ensure that any PHM technology’s performance and impact is accurately assessed. This breakout topic focused on assessing the performance of PHM along with the necessary technologies, measurement techniques, data, and performance metrics required for such verification and validation.

Breakout participants identified goals in the areas of identifying specific PHM performance characteristics and metrics, and equipment and technologies necessary to monitor a PHM system (or component). In addition, the participants also noted the long-term goal of incorporating the design and validation of a PHM system into the overall equipment/process life cycle. Once the participants identified the subsequent capabilities and existing challenges, six priority roadmap topics were developed. Three of the roadmaps are presented in detail while the remaining three (Cost Model for PHM Performance, Taxonomy of Applications, and Determination of PHM Data and Information Needs) are not presented due to space restrictions.

Overarching Architecture Framework for PHM with Standards and Key Performance Indicators (KPIs)

This roadmap was motivated by the participants’ acknowledgement that a PHM framework within multiple industries is either unclear or lacking in standards. This absence of standards promotes inconsistencies in PHM verification and validation.

The ultimate goal of this roadmap is to define a standard PHM architecture and create methods that will enable asset traceability and historical record keeping on PHM performance. To realize this goal, the participants identified the near-term action of benchmarking the current state of machine monitoring (starting with specific industries) and the mid-term tasks of cataloging the KPIs and mapping-out the typical diagnostic and prognostic trends (from the target industries). The vision is that this effort would produce a published catalog that gains some industry acceptance (100% acceptance is too ambitious at this time, yet an initial target was not determined). Likewise, international standards would be developed that are broad enough to cover a range of PHM implementations across multiple industries. These standards would have to be specific enough to guide manufacturers through the process of developing and implementing a means of verifying and validating their PHM capabilities. If successful, this roadmap is expected to have significant impact in improving equipment/process reliability, reducing costs, increasing industry's competitiveness, and enhancing maintenance scheduling.

Identification of PHM Performance Metrics

Participants produced this roadmap citing a lack of performance metrics capable of characterizing the value of prognostics to equipment or processes prior to failure. This coincides with limited information on key metrics for manufacturing equipment and/or processes at component and system levels. The overall approach proposed is to evaluate existing metrics to determine what metrics can be captured from equipment/processes prior to a fault or failure that sufficiently evaluate the performance of the PHM system in question. This assessment will aid in developing new performance metrics.

The near-term plans of this roadmap feature three activities: 1) survey current metrics that characterize the performance of a PHM system itself and the PHM's effectiveness when applied to a machine/process, 2) identify the necessary metrics that can apply diagnostics and prognostics to manufacturing equipment/process and integrate with controls/operations and maintenance planning, and 3) determine the gaps present between existing and desired metrics. Mid-term actions include 1) developing the missing metrics, 2) evaluating the metrics across a range of equipment, processes, systems, and PHM algorithms, and 3) studying how performance metrics can be integrated with controls, operations, and maintenance planning systems. Long-term activities conclude with integrating the identified performance metrics with the PHM architecture (described in the prior section) so the metrics can be implemented and demonstrating the applied metrics (in concert with the architecture) at selected pilot plants. The achievement of implementing the metrics and framework in a plant is envisioned to be a stepping-stone to applying the metrics and framework to additional manufacturing facilities.

The expected impact of completing this roadmap action plan includes better decisions being made based upon available PHM results and performance metrics; improved quality and productivity of equipment and processes; and greater availability of actionable information.

Failure Data for Prognostics and Diagnostics

The final roadmap is motivated by the lack of sufficient, available failure data for diagnostics and prognostics. Currently, measurement and data collection methods and appropriate test beds are limited in their availability and capability. For those methods and test beds that do exist, there is a lack of consistency in the data formats for which data is captured and organized. The participants who developed this roadmap proposed the approach of developing methods and services to generate diagnostic and prognostic data sets for public use including verification and validation. This would be supported by the development of specific test beds that would enable both the production of data and the necessary verification and validation.

The roadmap action plan begins with three near-term activities: 1) development of a common database, 2) creation of test beds to assess feasibility, and 3) establishment of a consortium (including NIST and university partners) to examine PHM for specific systems in the form of test bed(s). Mid-term activities include qualifying the data within the common database and further development of the scaled-down test beds. Long-term activities feature the implementation and testing of the common database, standardizing the scaled-down test beds, and performing simulation modeling of processes. Upon the completion of these tasks, the realized capabilities should be the active use of a common database and the adoption of PHM failure data standards. The realized impact of these capabilities is expected to include a significant reduction in cost (this method promotes cost sharing across the industry) and improved access to failure data to support verification and validation of PHM methods.

3.3.3. Breakout Topic: *PHM Infrastructure – Hardware, Software, and Integration*

Successful PHM methods and technologies require a robust infrastructure including key building blocks such as hardware, software, models, and simulations along with the integration of these elements. Technology has greatly advanced in the last decade (including enhanced capabilities in wireless connectivity, mobile devices, computing power, sensing capability, and human machine interfaces), and the PHM infrastructure has become increasingly complex. The participants in this breakout topic discussed a variety of infrastructure needs from the perspective of enabling and augmenting PHM within smart manufacturing environments.

Breakout participants identified near-term, mid-term, and long-term infrastructure goals in the areas of PHM design, hardware, software, security, maintenance, and data management. This prompted the participants to identify the capabilities and their corresponding priorities. Next, the participants identified the challenges and barriers to achieving these capabilities and prioritized them accordingly. These efforts led to the development of four roadmap action plans. Two of the roadmaps are presented in detail while the remaining two (PHM as an Equipment Design Feature and Embedded Sensors for PHM of Emerging Manufacturing Technologies) are not discussed due to space restrictions. Those roadmaps not discussed in this paper can be found in detail in the full workshop report (National Institute of Standards and Technology, 2015a).

Open-Source Community for PHM

The first roadmap action plan to be presented from this breakout topic is motivated by the fact that it is often costly and overly complex to implement PHM on new equipment. The proposed approach charts the path of developing an open source architecture that will reduce the cost and complexity of PHM design and implementation. The approach features a collection of data and identification of relevant PHM systems and devices.

The near-term activities of this roadmap include: 1) the development of open drivers and adapters enabling PHM through the integration of sensors, equipment, controllers, interfaces, etc. 2) the expansion of the data collection infrastructure to accommodate an open source format, and 3) the development of security, compression, fault tolerance, and schema for the open architecture. Mid-term tasks include: 1) identification of systems and devices to be compatible with the framework, 2) development of frameworks and toolkits to enable users to interface with equipment, and 3) expansion of drivers and adapters. Finally, the long-term task is a continuation of the prior tasks – promote continuous development and improvement (similar to what is done in the Linux community). The goal is to get a majority (ideally, all) of industry (ranging from small to large enterprises) using and contributing to the open architecture.

If this roadmap action plan is successfully completed, numerous impacts could be realized. The most significant impacts that could be realized include reduced individual cost to develop and implement PHM; accelerated pace of innovation since more time could be devoted to developing PHM algorithms as opposed to developing the architecture (since it would already be in place); and enhanced industrial competitiveness since the increased presence of PHM would reduce maintenance costs and enhance versatility.

PHM Infrastructure to Deliver Relevant Timely Information

The final roadmap action plan to be presented is similar to the roadmap highlighted in the last section, yet is still unique in scope and objectives. The participants developed this plan to overcome the current inability to make good decisions based upon the available data where PHM users are currently making decisions either with the wrong information, with insufficient detail, and/or at the wrong levels. The proposed approach focuses on developing a traffic light approach (e.g., green, yellow, red) to classifying the value of the data for decision-making.

This roadmap features an extensive action plan with eight near-term and six mid-term tasks identified. Some of the near-term tasks include the development of tools to construct cyber-models of replacement parts/components to better predict RUL or mean time to failure, determination of required data to model diagnostics and prognostics, and assess requirements to determine the necessary information needed at each operational level within a manufacturing environment. Several of the mid-term tasks include the development of a cloud-based data repository and analytic engine to further enhance decision-making and technology generation to enable adaptable alarms based upon equipment/process condition. The participants identified a single long-term goal – develop advanced usage-based models to augment PHM decision-making. Increased and enhanced decision-making is the ultimate desired capability where the participants envision 80% improvement (over existing baselines) after five years of effort on this roadmap.

The significant impacts that could potentially be realized if this action plan is completed are the generation and availability of better data for fault and failure prevention, and appropriate data and better decision-making are fused to make timely decisions regarding maintenance scheduling.

3.4. Cross-Cutting Themes

Over the entire course of the workshop, numerous themes emerged, both within the individual breakout topics and across the rest of the workshop program (plenary talks and panel discussions). Six specific themes were identified; three are presented in the following sub-sections while the other three (Workforce and Training, Human Factors, and Business Case for PHM) are not presented.

3.4.1. Data Collection and Extraction of Information

The challenges of collecting, extracting, and analyzing appropriate and meaningful data were well documented throughout the workshop. Data is a critical piece of designing, verifying, validating, and implementing effective PHM technologies into a manufacturing process or piece of equipment. These challenges stem from a lack of sensors capable of capturing the right data at the appropriate frequency, accuracy, and resolution; and a lack of rigorous measurement methods to enable efficient and effective data collection methods suited for PHM. Additionally, inconsistent or insufficient data standards are making it difficult to broadly apply PHM across a range of manufacturing equipment and processes; standardization of data formats and taxonomies would play a significant role in overcoming this challenge. Another data challenge is generating accurate PHM data, for the purposes of PHM design, verification, and validation without damaging equipment or decreasing productivity.

3.4.2. Models, Simulation, and Visualization

Validated models to support PHM are limited in availability and capability. The entire scope of modeling, simulation, and visualization (MSV) is also encumbered by the diversity of manufacturing equipment and processes, lack of integration with legacy systems, and data availability (which is critical for effective MSV). A benefit of having accurate and relevant models is that they can help highlight the value of PHM prior to a system being put into practice. This would help generate further organizational support for PHM, and it sets initial expectations of the predicted performance.

3.4.3. Design Considerations

The last cross-cutting theme to be highlighted is the notion that PHM be considered as a design feature that is factored in to the design process of any new piece of manufacturing equipment or process. Most original equipment manufacturers (OEMs) do not consider PHM in their design process; any PHM that is factored typically include limited forms of condition-monitoring and diagnostics. Likewise, most technology integrators will not add PHM into their process design unless their customer specifically requests PHM and is willing to pay the additional costs for it. It is much more challenging to integrate effective PHM into a system/process after that system/process is in service on a factory floor.

4. NIST'S RESEARCH DIRECTION

The workshop provided valuable insight that is envisioned to bring tremendous benefit to the PHM community. Likewise, NIST is carefully reviewing the workshop findings to update its project's research direction to further align it with industry's needs and high priorities. The PHM4SMS project team is currently focused on four specific efforts that are all factoring in the workshop findings.

4.1. Machine Tool Linear Axes Diagnostics

This effort is focused on developing a sensor-based method to quickly estimate the degradation of linear axes, and is supported by the development of a linear axes test bed. This method leverages data collected from a NIST-developed sensor suite to detect translational and angular changes due to axis degradation. Real-time data is collected to enable diagnostics and prognostics of linear axes for optimization of maintenance scheduling and part quality. This method to estimate the degradation of linear axes will also enable verification and validation of other (built-in or otherwise) PHM techniques that aim to characterize translation and angular errors and degradation. Likewise, this method will produce reference data sets that can be used by PHM developers as test data so they do not have to risk damaging their own equipment or impacting their productivity. This method will ultimately lead to standards to measure and predict linear axes degradation. The linear axes test bed will yield its first data sets for analysis in Summer 2015.

4.2. Manufacturing Process and Equipment Monitoring

Driven by the need to identify high-value data sources and the most appropriate times to collect data, this manufacturing process and equipment monitoring effort focuses on enabling the seamless and effective use of data to generate timely and actionable intelligence on equipment/process health. This effort is supported by the development of a systems-level test bed of networked machine tools and sensors in an active manufacturing facility. Accordingly, a significant part of this research is the design of a reference implementation that manufacturers may use to collect data safely and efficiently without disruption to operations. Likewise, this effort will also yield a reference dataset of fabrication and inspection data that may be used to identify useful links for improved process monitoring, diagnostic, and prognostic capabilities. This test bed will produce initial results in Fall 2015.

4.3. Systems-Level Diagnostics and Prognostics

Many complex processes and systems-of-systems are lacking in higher-level capabilities to accurately and efficiently forecast faults and failures. This research effort addresses this challenge by developing protocols to communicate data, information and metrics across the component, sub-system, and system levels for diagnostics and prognostics in manufacturing. These protocols will enable the prediction of system-level impacts of events occurring at a single component or sub-system. Moreover, the protocols will enable and enhance process management and control approaches to effectively respond to these events. A hierarchical methodology is being developed with external partners, and will be applied to the two aforementioned test beds in 2016.

4.4. PHM for Robotics

Robotics are increasing in their implementation and complexity of integration within manufacturing operations. PHM considerations of a robotic system extend beyond just the physical arm, gantry, mobile base, etc. nearly every robotic system features some type of end-effector, sensors, safety system(s), supporting/surrounding automation, controller, etc. Robotic systems, especially in smart manufacturing environments, are often marked by complex interactions among these elements. For example, a fault or failure that presents itself as unexpected or inappropriate behavior of the robot arm is likely to have resulted not from a mechanical failure of the arm, but rather from a failure elsewhere in the system (e.g., sensor failure, or a controller fault). This research effort is actively developing a PHM-focused robotics test bed that features a scaled-down industrial robotic arm system to develop test methods, metrics, assessment protocols, and reference data sets that can evaluate robot system degradation techniques including how such degradation impacts key elements of the robot system (e.g., safety). This test bed is expected to be operational and produce its first data sets in Summer 2016.

5. CONCLUSION

The two-day workshop brought together many PHM experts who shared their best practices, challenges, and visions with respect to PHM in smart manufacturing (National Institute of Standards and Technology, 2015a). Their extensive feedback is well-documented in the roadmap action plans, and will guide the community in devising and updating their research directions, accordingly. As a member of the community, NIST is examining the workshop findings to best determine where its research efforts can have substantial impact in addressing PHM measurement science challenges.

ACKNOWLEDGEMENT

The authors would like to thank the workshop speakers, panelists, and participants for their focused and diligent efforts during the two-day event. Their willingness to share their PHM experiences and vision made this report possible.

DISCLAIMER

The views and opinions expressed herein do not necessarily state or reflect those of NIST. Certain commercial entities, equipment, or materials may be identified in this document in order to illustrate a point or concept. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

REFERENCES

Ahmad, R. & Kamaruddin, S. (2012). An overview of time-based and condition-based maintenance in industrial application. *Computers & Industrial Engineering*, vol. 63(1), pp. 135-149.

Barajas, L. G. & Srinivasa, N. (2008). Real-time diagnostics, prognostics health management for large-scale manufacturing maintenance systems. *ASME International Manufacturing Science and Engineering Conference, MSEC2008* (pp. 85-94), Evanston, IL, United States. doi: 10.1115/MSEC_ICMP2008-72511

Bernaden, J. (2012). *Indirect jobs: A direct way to talk about why we need smart manufacturing.* Rockwell Automation.

Butcher, S. W. (2000). *Assessment of condition-based maintenance in the Department of Defense.* Logistics Management Institute, McLean, Virginia.

Byington, C. S., Roemer, M. J., Kacprzymki, G. J., & Galie, T. (2002). Prognostic enhancements to diagnostic systems for improved condition-based maintenance. *2002 IEEE Aerospace Conference* (pp. 2815-2824), Big Sky, MT, United States. doi: 10.1109/AERO.2002.1036120

Coats, D., Hassan, M. A., Goodman, N., Blechertas, V., Shin, Y.-J., & Bayoumi, A. (2011). Design of advanced time-frequency mutual information measures for aerospace diagnostics and prognostics. *2011 IEEE Aerospace Conference, AERO 2011*, Big Sky, MT, United States. doi: 10.1109/AERO.2011.5747575

Kothamasu, R., Huang, S. H., & VerDuin, W. H. (2006). System health monitoring and prognostics - a review of current paradigms and practices. *The International Journal of Advanced Manufacturing Technology*, vol. 28, pp. 1012-1024.

Lee, J., Ni, J., Djurdjanovic, D., Qiu, H., & Liao, H. (2006). Intelligent prognostics tools and e-maintenance. *Computers in industry*, vol. 57(6), pp. 476-489.

Lee, J., Ghaffari, M., & Elmeligy, S. (2011). Self-maintenance and engineering immune systems: Towards smarter machines and manufacturing systems. *Annual Reviews in Control*, vol. 35(1), pp. 111-122. doi: 10.1016/j.arcontrol.2011.03.007

Manyika, J., Sinclair, J., Dobbs, R., Strube, G., Rassey, L., Mischke, J., Remes, J., Roxburgh, C., George, K., O'Halloran, D., & Ramaswamy, S. (2012). *Manufacturing the future: The next era of global growth and innovation*: McKinsey Global Institute.

Montgomery, N., Banjevic, D., & Jardine, A. K. S. (2012). Minor maintenance actions and their impact on diagnostic and prognostic CBM models. *Journal of Intelligent Manufacturing*, vol. 23(2), pp. 303-311. doi: 10.1007/s10845-009-0352-0

Muller, A., Crespo Marquez, A., & Iung, B. (2008). On the concept of e-maintenance: Review and current research. *Reliability Engineering & System Safety*, vol. 93(8), pp. 1165-1187.

National Institute of Standards and Technology (2015a). *Measurement Science Roadmap for Prognostics and Health Management for Smart Manufacturing*

Systems: http://www.nist.gov/el/isd/upload/Measurement-Science-Roadmapping-Workshop-Final-Report.pdf

National Institute of Standards and Technology (2015b). *Roadmapping Workshop on Measurement Science for Prognostics and Health Management of Smart Manufacturing Systems Agenda*: http://www.nist.gov/el/isd/phm4sms-workshop-agenda.cfm

PCAST (2012). *Report to the President: Capturing Domestic Competitive Advantage in Advanced Manufacturing.* Executive Office of the President - President's Council of Advisors on Science and Technology.

PCAST (2014). *Report to the President: Accelerating U.S. Advanced Manufacturing.* Executive Office of the President - President's Council of Advisors on Science and Technology.

Peng, Y., Dong, M., & Zuo, M. J. (2010). Current status of machine prognostics in condition-based maintenance: A review. *The International Journal of Advanced Manufacturing Technology*, vol. 50(1-4), pp. 297-313.

Tian, Z., Lin, D., & Wu, B. (2012). Condition based maintenance optimization considering multiple objectives. *Journal of Intelligent Manufacturing*, vol. 23(2), pp. 333-340. doi: 10.1007/s10845-009-0358-7

Vogl, G. W., Weiss, B. A., & Donmez, M. A. (2014a). *Standards related to prognostics and health management (PHM) for manufacturing.* National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, USA, NISTIR 8012. doi: 10.6028/NIST.IR.8012

Vogl, G. W., Weiss, B. A., & Donmez, M. A. (2014b). Standards for prognostics and health management (PHM) techniques within manufacturing operations. *Annual Conference of the Prognostics and Health Management Society 2014*, Fort Worth, Texas, USA.

Zhou, Y., Bo, J., & Wei, T. (2013). A review of current prognostics and health management system related standards. *Chemical Engineering Transactions*, vol. 33, pp. 277-282. doi: 10.3303/CET1333047

BIOGRAPHIES

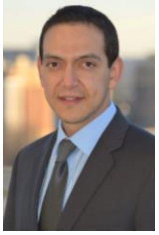
Dr. Brian A. Weiss has a B.S. in Mechanical Engineering (2000), Professional Masters in Engineering (2003), and Ph.D. in Mechanical Engineering (2012) from the University of Maryland, College Park, Maryland, USA. He is currently the Associate Program Manager of the *Smart Manufacturing Operations Planning and Control (SMOPAC)* program and the Project Leader of the *Prognostics and Health Management for Smart Manufacturing Systems (PHM4SMS)* project within the Engineering Laboratory (EL) at NIST. Prior to his leadership roles in the SMOPAC program and the PHM4SMS project, he spent 15 years conducting performance assessments across numerous military and first response technologies including autonomous unmanned ground vehicles; tactical applications operating on Android™ devices; advanced soldier sensor technologies; urban search and rescue robots; and bomb disposal robots. His efforts have earned him numerous awards including a Department of Commerce Gold Medal (2013), Silver Medal (2011), Bronze Medals (2004 & 2008), and the Jacob Rabinow Applied Research Award (2006).

Dr. Gregory W. Vogl is a Mechanical Engineer at NIST. He received his B.S. (2000), M.S. (2003), and Ph.D. (2006) degrees in Engineering Mechanics from Virginia Tech, Virginia, USA. Currently, Greg is a member of the *Prognostics and Health Management for Smart Manufacturing Systems* (PHM4SMS) project, which seeks to develop a methodology, protocols, and reference datasets to enable robust real-time diagnostics and prognostics for smart manufacturing systems. Previously, he designed, fabricated, and experimented on microelectromechanical systems as a National Research Council Postdoctoral Researcher at NIST. He then joined the Production Systems Group, in which he worked on machine tool metrology and standards development. His interests include machine tool spindle health, diagnostic and prognostic methods, nonlinear dynamics, engineering mechanics, and metrology.

Dr. Moneer Helu is a mechanical engineer in the Engineering Laboratory at NIST where his research currently focuses on performance assurance and prognostics and diagnostics for smart manufacturing systems. Prior to joining NIST in 2014, he was the Associate Director of the Laboratory for Manufacturing and Sustainability and a Lecturer in the Department of Mechanical Engineering at UC Berkeley. He received his Ph.D. from UC Berkeley and has been recognized by the Society of Manufacturing Engineers in the 2014 list of the "30 Under 30: Future Leaders of Manufacturing."

Dr. Guixiu Qiao is a mechanical engineer at the NIST. She is a member of the PHM4SMS project, focusing on PHM for robotic systems. She has 12+ years' experience in high precision industry, expertise in advanced sensors, automation, manufacturing, and information integration; with a strong background in algorithms and optimization. She is a 2011 R&D 100 award winner for "3D volumetric accuracy error compensation for large machine tool" recognizing the most technologically-significant products introduced into the marketplace; 2009 recipient of the Defense Manufacturing Excellence award for the contribution of pioneering efforts in volumetric accuracy for large machine tools; and a 2003 recipient of Boeing's Exceptional Performance award. Dr. Qiao holds her Ph.D. in robotics from the Robot Research Institute, Harbin Institute of Technology, China.

Joan Pellegrino is Vice President of Energetics' Science and Technology Division. She has more than 27 years of experience analyzing advanced industrial technologies, conducting cost/benefit analysis, assessing broad energy and environmental trends/statistics, and evaluating bioenergy systems. She has also worked with NIST for over 15 years assessing the strategic measurement science and metrology needs of external stakeholders across the Nation. Her broad experience includes strategic planning, technology roadmapping, market intelligence and business planning, technology transfer, and stakeholder engagement/ community building. She has worked with a diversity of government agencies, academic institutions, national laboratories, state/local governments, and commercial entities and provides high-level technical and management advising. Ms. Pellegrino is a professional facilitator with experience designing effective stakeholder engagements; she has contributed to over 80 strategic plans and technology roadmaps on a variety of technical topics. She holds a M.S. in Chemical Engineering from Auburn University and a B.S. in Chemical Engineering from the University of Tennessee, Knoxville.



Mauricio Justiniano is a Senior Engineer at Energetics with over 15 years of experience in energy and environmental consulting. He specializes in project management of technology deployment projects, such as smart grid technologies, and benefits analysis of emerging technologies. Mauricio is an experienced strategic planning consultant helping diverse clients develop visionary strategies, prioritize investments, and devise solutions to complex problems. Prior to joining Energetics, he was a consultant for the World Bank Group's International Finance Corporation where he researched technology investment opportunities and the economic environment of potential loan-recipient countries and industrial sectors. Mauricio is a Certified Project Management Professional (PMP), and has a MS in Finance from Johns Hopkins University and a BS in Mechanical Engineering from the University of Maryland – College Park.

Anand Raghunathan is a senior materials engineer at Energetics Incorporated. As a consultant to NIST, U.S. Department of Energy (DOE), and private-sector clients, he works on technology, strategy, and program management activities with various groups that include creating long-range, strategic roadmaps. While at Booz Allen Hamilton and the Schafer Corporation, he worked with program managers at the Defense Sciences, Microsystems Technology, and Strategic Technology Offices within the U.S. Department of Defense's Defense Advanced Research Projects Agency to identify and advance relevant high-risk/high-reward technologies to protect national interests. As an engineer at 3M and Chorum Technologies, Anand worked on materials and telecommunications technologies across the phases of the product development cycle—conducting research and development, designing specifications with global customers, optimizing manufacturing processes, and securing sales. Anand has BS and MS degrees in materials science and engineering from the Massachusetts Institute of Technology.

Use Case Development to Advance Monitoring, Diagnostics, and Prognostics in Manufacturing Operations

Brian A. Weiss, Moneer Helu, Gregory Vogl, Guixiu Qiao

National Institute of Standards and Technology, Gaithersburg, MD 20899
USA (Tel: 301-975-4373; e-mail: brian.weiss@nist.gov,
moneer.helu@nist.gov, gregory.vogl@nist.gov, guixiu.qiao@nist.gov).

Abstract: Manufacturing operations suffer from degradation as equipment and processes are continually used to generate products. The development and integration of monitoring, diagnostic, and prognostic (collectively known as PHM) technologies can enhance maintenance and control strategies within manufacturing operations to improve asset availability, product quality, and overall productivity. As these technologies continue to evolve, it is critical for PHM technologies to be assessed to ensure the manufacturing community is aware of the true capabilities and potential of PHM technologies. The National Institute of Standards and Technology (NIST) has developed a use case that is representative of common manufacturing operations to support the assessment of PHM technologies. This use case will produce test scenarios, reference data sets and protocols, and verification and validation tools. The use case is described including its three constituent research areas: *Manufacturing Process and Equipment Monitoring*, *Machine Tool Linear Axes Diagnostics and Prognostics*, and *Health and Control Management of Robot Systems.*

Keywords: diagnostics, manufacturing processes, manufacturing systems, condition monitoring, prognostics, use cases

1. INTRODUCTION

Advanced technology continues to emerge and evolve leading to increasing capabilities within manufacturing operations. Smart Manufacturing or Industrie 4.0 are focused on integrating and connecting hardware, software, and data to increase operational efficiency, asset availability, and quality while decreasing unscheduled downtime and scrap (Kagermann et al., 2013) (McKinsey, 2012) (PCAST, 2012). This translates into manufacturing operations becoming more efficient to keep up with changing consumer demand and increasing competition.

Asset availability is critical for manufacturers to output products to meet consumer demand. Unexpected downtime and lost production are ‘pain points’ for manufacturers, especially in that they usually translate to financial losses. To minimize these pain points, the manufacturing stakeholder community (including manufacturers, technology developers, integrators, and academic researchers) are advancing monitoring, diagnostic, and prognostic (commonly known as prognostics and health management - PHM) technologies to improve maintenance and control strategies.

The United States (U.S.) Federal Government has a research focus in advancing the means of assessing, verifying, and validating PHM technologies operating within manufacturing environments (National Institute of Standards and Technology, 2016). This effort resides at the National Institute of Standards and Technology (NIST) and includes a focus on machine tool and robotic manufacturing operations. NIST researchers are actively developing use cases, performance metrics, test protocols and reference data sets to enable the verification and validation (V&V) of PHM technologies.

2. BACKGROUND

The need for PHM is motivated by the fact that as soon as you turn on a piece of equipment or initiate a process (requiring the interaction of one or more physical entities), the system begins to degrade, ultimately causing ‘wear & tear.’ If unchecked, this degradation will lead to faults or failures impacting the overall quality and/or productivity of the process. The field of PHM has emerged from the study, design, and implementation of monitoring, diagnostic, and/or prognostic technologies to minimize the occurrence of failures. PHM aims to increase our knowledge of a process so that one can make better maintenance and control decisions.

2.1 Manufacturing Health and Control Management

Four maintenance strategies have been documented and applied in varying extents across the manufacturing environment. The strategies are known as reactive, preventative, predictive, and proactive maintenance (Jin et al., 2016). Reactive maintenance is the simplest form of maintenance; no maintenance is performed on the machine until a failure occurs. Although this maintenance strategy is the easiest to implement (i.e., do nothing until something breaks), it is often the most expensive strategy when considering maintenance costs, lost asset availability, lost production, and potential collateral damage. Preventative maintenance is when maintenance is performed on specific unit intervals (e.g., x cycles, y hours) and is widely performed in the manufacturing industry (Ahmad and Kamaruddin, 2012) (Coats et al., 2011). Predictive maintenance, sometimes known as condition-based maintenance, uses health and/or performance data captured from the equipment or process to indicate when maintenance should be performed (Byington et al., 2002) (Tian et al., 2012). There are instances of manufacturers using predictive maintenance strategies within their operations, yet this is typically incorporated in areas where data collection, and subsequent analysis, is feasible and there is a known value proposition to such a strategy. Proactive maintenance, sometimes known as intelligent maintenance, is an emerging strategy that relies upon data collection from the manufacturing process to improve and sustain the process, in addition to minimizing the occurrence of failures (Barajas and Srinivasa, 2008) (Lee et al., 2011) (Lee et al., 2006). Proactive maintenance is unique from other maintenance strategies in that it is marked by varying levels of equipment or process intelligence in terms of maintenance and control activities. Equipment or processes have some capability(ies) in performing certain maintenance activities until an appropriate human intervention can be achieved or until specific production objectives are met. Proactive maintenance is the most advanced of the maintenance strategies and is minimally employed given its state of development. Aside from implementing reactive maintenance, the implementation of preventative, predictive, and/or proactive maintenance will lead to improved health and control management of a piece of equipment or an overall process.

Apart from reactive maintenance, these maintenance strategies are each supported by monitoring, diagnostics, and prognostics (to a certain extent). Monitoring is the act of identifying, observing, or understanding the current health state of equipment or a process. Diagnostics is the determination of what is going to fail and, depending upon the system, where the failure will occur. Prognostics is the determination of the future state of the equipment or process. Prognostics is also responsible for predicting the remaining useful life (RUL) of equipment or a process (Ly et al., 2009).

The advancement of monitoring, diagnostic, and prognostic technologies has increased the development and implementation of preventative, predictive, and proactive maintenance strategies. A wide range of techniques, algorithms, and practices have been developed with varying success (Vogl et al., 2016b). Not only has PHM enhanced maintenance strategies, but it has also promoted more intelligent control of processes. Some monitoring, diagnostic, and prognostic techniques feed adaptive control strategies allowing processes to automatically adjust their performance (or output) given their current state of health (Ehrmann and Herder, 2013, Liu, 2001) (Shin and Lee, 1999). These control strategies are limited and have room for expansion.

2.2 Manufacturing Case Studies

According to the manufacturing and PHM communities, there is still much work to be done to improve monitoring, diagnostic, and prognostic practices to enhance maintenance and control strategies. NIST personnel conducted manufacturing case studies to understand the current successes and challenges to developing and implementing PHM within manufacturing operations. This information was gathered by having representatives of the manufacturing community come to NIST or by NIST personnel directly reaching out to manufacturers via phone calls or site visits.

A workshop was held at NIST that brought together small, medium, and large-sized manufacturers along with technology developers, technology integrators, academia, government, and standards development organizations to examine the challenges and barriers to advancing the state of PHM within manufacturing operations. This workshop resulted in the generation of a substantial roadmapping document that highlighted over a dozen research topics that should be undertaken to enhance the state of PHM (National Institute of Standards and Technology, 2015). The workshop presented some trends across multiple manufacturers as far as areas for improvement. Some of the common themes included the manufacturing community's desire to 1) better understand and integrate advanced sensing capabilities into equipment and processes to increase PHM, 2) identify a suite of common PHM performance metrics that would present a holistic understanding of equipment or process health, and 3) generate/access larger volumes of structured and contextualized failure data for prognostics and diagnostics to promote further maintenance strategy development (Weiss et al., 2015).

NIST personnel, and their collaborators from the University of Cincinnati and the University of Michigan – Ann Arbor, spoke/met with over 30 manufacturers representing small to medium-sized enterprises (SMEs) and large companies (Helu and Weiss, 2016) (Jin et al., 2016). Many trends, including similarities and differences, were documented between SMEs and large companies. One similarity that stands out is that no single organization used the same maintenance strategy across all of its equipment and processes. For example, some companies employed a mix of reactive and preventative maintenance strategies, while other companies employed a mix of preventative and predictive maintenance with minimal reactive maintenance. One of the biggest differences between SMEs and large companies is that an overwhelming majority of the large companies are more advanced in their maintenance strategies as compared to the SMEs. This can be attributed to the greater resources available to the large companies including more financial capital and available personnel. These manufacturing case studies also revealed some common scenarios in which implementing or increasing PHM would be beneficial to a process' asset availability, output quality, and overall productivity.

3. USE CASE DEVELOPMENT

It is imperative to generate appropriate use cases to produce test scenarios, reference datasets and protocols, and V&V tools that allow technology developers and integrators to address the manufacturing community's needs and promote the evaluation of various technology options. Six areas for theoretically impactful use cases emerged from the case studies:

- Planning and scheduling support
- Maintenance planning and spare part provisions
- Request for proposals
- Resource budgeting (e.g., capital investments)
- Workforce augmentation
- Automation

NIST personnel identified an initial use case that would feature several of the six areas mentioned above, represent a manufacturing operation common in numerous organizations, and also present numerous individual elements prevalent within many manufacturing environments. This case study (depicted in Fig. 1) presents a production work cell containing representative systems common in modern manufacturing facilities, including computer numeric control (CNC) machine tools and a six-degree-of-freedom (6-DOF) industrial robot arm. The concept of operations is that materials and resources are input into the cell and are dynamically routed to one or more machines based upon the current and predicted status of the machine tools, their components, and the robot manipulating the parts. The use case features the robot performing machine tending by first presenting a machine tool with a part to be machined and then removing the part from the machine tool once the machining operations have been completed. These elements would be coordinated with each other based on the quantified state of all components by a principal control system. This control system would route materials dynamically based on the measured state and performance of the system as well as input from design, engineering, suppliers, and other actors across the manufacturing enterprise (Helu and Weiss, 2016).

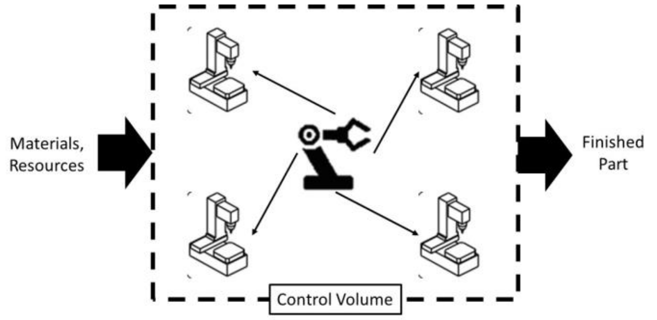


Fig. 1. NIST Use Case Production Cell

Other use cases are being considered, including 1) multiple 6-DOF industrial robot arms assembling parts after the parts have been machined by one or more machine tools and 2) a 6-DOF industrial robot arm moving machined parts from a conveyor to a fixture so that another 6-DOF industrial robot arm may ‘mark’ the fixture part. Each of these use cases, including the initial use case, are being carefully chosen to represent a majority of the machine tool and robot system scenarios that were encountered during the case studies and documented during the NIST workshop.

The initial use case is designed such that it is relevant to industry, allows for the practical implementation of NIST’s research efforts, and can be supported by NIST’s test beds. Use case implementation has begun with several of NIST’s research efforts. Specifically, these efforts (presented in sections 4 and 5) highlight key elements that will ultimately be integrated together via the use case.

4. USE CASE IMPLEMENTATION

The initial use case described in Section 3. is currently broken down into three key research elements: *Manufacturing Process and Equipment Monitoring*, *Machine Tool Linear Axes Diagnostics and Prognostics*, and *Health and Control Management of Robot Systems*.

4.1 Manufacturing Process and Equipment Monitoring

The *Manufacturing Process and Equipment Monitoring* research effort is aimed at monitoring the overall health of a manufacturing shop floor including the health of resident machine tools. This effort is driven by the need to identify high-value data sources and the most appropriate opportunities to collect data to avoid the challenges of big data. The focus is on having the right data at the right time to improve decision-making with respect to process and equipment performance. This research is supported by the development of a systems-level test bed of networked machine tools and sensors in an active manufacturing facility (Helu and Hedberg, 2015). The test bed provides a valuable testing and prototyping environment replete with rich data to support fundamental research, technology, and standards development. This research area will focus on integrating heterogeneous shop-floor systems through the development and advancement of standards and protocols. Specifically, the task will integrate sensors (including accelerometers, cameras, and thermocouples), machine tool controllers, and production management systems. Initial standards research focuses on the extension of MTConnect across manufacturing equipment and systems.

This research encompasses a substantial portion of the initial use case. The test bed includes a heterogeneous mix of machine tools with different capabilities and operating on varying controllers, that must effectively function in the same environment to meet the shop’s overall production schedule. The defined use case includes multiple machine tools that will be called upon to perform a range of operations to fabricate specific parts. Until the robotics portion of the use case is integrated, parts will be placed and removed within the machine tools by human operators.

The test bed is currently online and streaming publicly available data from several machine tools that are in regular use by NIST Fabrication Technology machine shop personnel (Hedberg and Helu, 2016). The online data stream is provided using data formats defined in the MTConnect standard. Additional sensors are integrated with many of the machine tools to capture more data that can provide greater clarity on individual machine and overall process health. One such sensor that is being integrated with the test bed, and therefore the use case, is that of a novel sensor fusion device that generates error data of machine tool linear axes.

4.2 Machine Tool Linear Axes Diagnostics and Prognostics

Most information that is viewed at the shop-floor level originates from a lower level. These lower levels include the process, equipment, and component levels. Focusing on machine tools, there are numerous components that are prone to faults and failures throughout a machine tool's life that should be monitored to minimize unplanned downtime. Axis degradation is a reality of machine tools; monitoring axis health can also promote greater asset availability. Accurately detecting degradation of linear axes is typically a manual and time-consuming process. While direct methods for machine tool performance evaluation are well-established (International Organization for Standardization, 2012) and reliable for position-dependent error quantification, such measurements typically interrupt production (Khan and Chen, 2009). One potential solution for online monitoring of linear axis degradation is the use of an inertial measurement unit (IMU) (Vogl et al., 2015).

As seen in the schematic (Fig. 2), an IMU is mounted to a moving machine tool component. To diagnose axis degradation, the axis is moved back and forth at various speeds to capture data for different frequency bandwidths. This data is then 'fused' to estimate the changes in the 6-DOF geometric errors of the axis. Ideally, data would be collected periodically to track axis degradation with minimal disruptions to production. With robust diagnostics and prognostics algorithms, incipient faults may be detected and future failures may be avoided. This research supports the use case by offering another component-level sensor suite and methodology to monitor machine tool health. Prior to integrating this novel IMU into the larger shop floor test bed and the use case, it is critical that the methodology go through initial testing, independently of any machine tools.

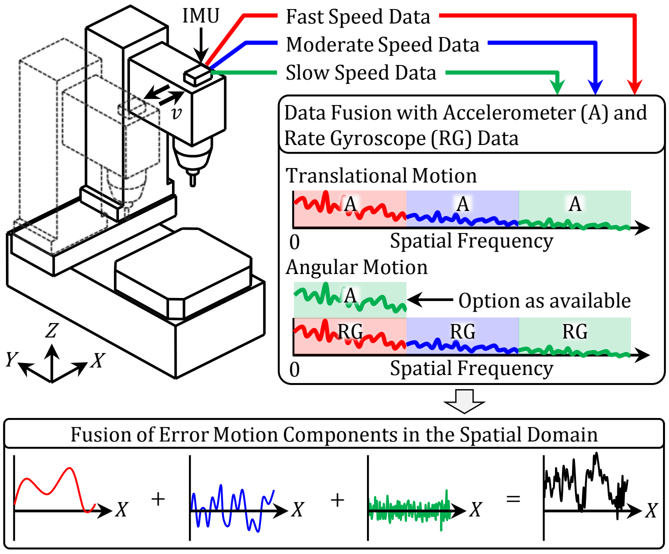


Fig. 2. IMU-based method for diagnostics of machine tool performance degradation.

A test bed was designed for evaluation of the IMU-based method. As seen in Fig. 3, the test bed includes a translation stage, the IMU, a commercial laser-based system for measuring the geometric errors of the axis, and a direct current (DC) motor with encoder for motion control. While the metrology system measures the motion of the carriage with respect to the base of the linear axis, the carriage-mounted IMU measures the changes in the inertial motion of the carriage. The metrology system measures straightness and angular error motions over the travel length of 0.32 m with standard uncertainties of 0.7 µm and 3.0 µrad. The laser-based system is used for verification and validation (V&V) of the IMU-based results.

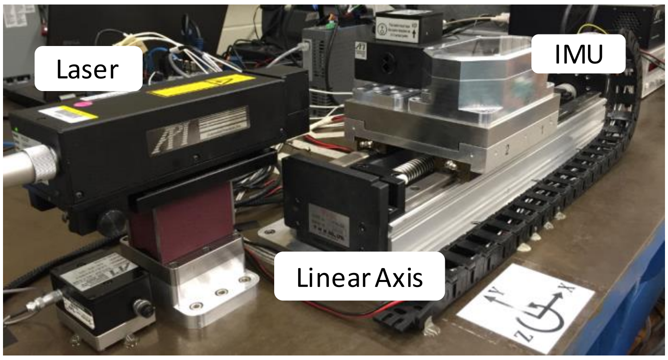


Fig. 3. Linear axis testbed

The IMU-based method relies on fusion of data collected at three programmed speeds of the carriage. The different speeds allow for sensing of repeatable error motions, composed of low to high spatial frequencies, within different temporal bandwidths. (Vogl et al., 2016a). Each 'run' is composed of data collected at the three axis speeds, and the resulting error motions per run are averaged to produce the final IMU-based error motions.

Typical laser-based and IMU-based results averaged for 50 runs are compared against one another to evaluate the methodology. The standard deviations of the differences are 11 µm, 2.3 µm, and 13 µrad for the linear positioning, straightness, and angular error motions, respectively. Due to the smallness of the deviations, the IMU-based method may be used for the estimation of changes in geometric motion errors of linear axes. Consequently, IMU data can be used to help optimize maintenance of machine tools for improved production planning and ultimately part quality.

4.3 Health and Control Management of Robot Systems

Similar to a machine tool, a robot system will begin to degrade from the moment it is put into operation. Although a 6-DOF industrial robot arm may be relatively robust, the robot system is a different story, altogether. The robot system includes the arm, end-effector, sensors, controller(s), safety systems, supporting automation, and human machine interface (HMI). Not only is each one of these elements susceptible to certain failures, the integration of these components and formation of specific relationships can increase the pace of degradation and lead to a cascade of failures.

The robot system is a key element of the initial use case defined in Section 3. To successfully accomplish its machine tending operations within the use case, the robot system must be aware of each machine tool's status that it intends to interact, aware of its own status (e.g., its current health and position), and aware of its environment (e.g., presence of an operator in its work volume). Without monitoring, diagnostics, and prognostics, a robot system will effectively function for a limited amount of time before it is likely to experience a fault or failure.

A robot systems test bed is under construction to support a framework for the assessment of monitoring, diagnostic, prognostic, and control technologies. The test bed will serve as the home to several industrial robot arm systems and will promote the generation of test methods and datasets. Advanced sensing and data collection techniques (what information to collect, how to collect, sensors to use, etc.) will be developed. Reference datasets will be generated to offer researchers and manufacturers a means of verifying and validating their diagnostic and prognostic techniques without the need for their own physical implementations. Reference data processing algorithms (data synchronization, data fusion of multiple sensor streams, and PHM data formats for interoperability) will be developed to analyze the PHM data that assesses the robot system's health metrics. This will support the closed-loop framework with the inclusion of diagnostic and prognostic techniques to promote better decision making for updating maintenance and control strategies.

5. FUTURE WORK

Each of the three research areas presented in Section 4. are in various phases of development and will ultimately be integrated together to form the defined use case. Efforts are under way to increase the data output from the Smart Manufacturing Systems Test Bed from two machine tools to approximately ten within the *Manufacturing Process and Equipment Monitoring* research. This will increase the publicly available volatile data stream and offer greater data sets to further support use case development. Besides getting additional machine tools online, more sensors are being planned for integration. Near term additions include power meters and the IMU sensor box presented in Section 4.2. The IMU sensor box design has been further refined from its original design to present a smaller profile when mounted to the axes of a machine tool. It is expected that the IMU sensor box will be mounted to a NIST machine tool in late 2016 so that it will capture linear axes error data during a pre-defined start-up sequence (at minimum) and during cutting operations (ideally). This data will be compared against machine tool controller data, including planned and actual data from the controller.

The *Health and Control Management of Robot Systems* effort will continue to evolve. To support the initial use case, a quick health assessment methodology is being developed to identify the health of the robot system, with an emphasis on a subset of the robot health performance metrics – tool center point accuracy and accuracy of tool center velocity. This effort will allow manufacturers to quickly assess the positional health of their robot systems when environmental conditions change, or after a work cell has been reconfigured. In turn, this methodology can also enable manufacturers and technology developers to verify and validate their own PHM techniques that monitor robot health in terms of static and dynamic accuracy. Further evolution of this effort will continue in the form of adding more sensors to monitor robot health, position, and environmental conditions/parameters. Likewise, the complexity of the robot system will be increased with the inclusion of an end-effector and supporting automation (e.g., conveyor belts to present parts to the robot arm).

6. CONCLUSION

An initial use case is documented that originates from feedback received from SME and large manufacturers. This use case provides an opportune breeding ground to develop test methods, reference data sets and protocols, and V&V tools to promote the assessment of monitoring, diagnostic, and prognostic techniques. These PHM techniques have been identified by the manufacturing community as necessary research areas to advance and promote more intelligent maintenance and control strategies. NIST is contributing to the overall PHM research field in the development of this use case to include three key research areas: *Manufacturing Process and Equipment Monitoring*, *Machine Tool Linear Axes Diagnostics and Prognostics*, and *Health and Control Management of Robot Systems.* Individually, and together, each of these research areas represents common operations whose degradation and overall health need to be understood to promote sustained, efficient manufacturing.

NIST DISCLAIMER

The views and opinions expressed herein do not necessarily state or reflect those of NIST. Certain commercial entities, equipment, or materials may be identified in this document in order to illustrate a point or concept. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

REFERENCES

AHMAD, R. & KAMARUDDIN, S. 2012. An overview of time-based and condition-based maintenance in industrial application. *Computers & Industrial Engineering*, 63**,** 135-149.

BARAJAS, L. G. & SRINIVASA, N. Real-time diagnostics, prognostics health management for large-scale manufacturing maintenance systems. ASME International Manufacturing Science and Engineering Conference, MSEC2008, 2008 Evanston, IL, United States. ASME Foundation, 85-94.

BYINGTON, C. S., ROEMER, M. J., KACPRZYMKI, G. J. & GALIE, T. Prognostic enhancements to diagnostic systems for improved condition-based maintenance. 2002 IEEE Aerospace Conference, 2002 Big Sky, MT, United States. IEEE Computer Society, 2815-2824.

COATS, D., HASSAN, M. A., GOODMAN, N., BLECHERTAS, V., SHIN, Y.-J. & BAYOUMI, A. Design of advanced time-frequency mutual information measures for aerospace diagnostics and prognostics.

2011 IEEE Aerospace Conference, AERO 2011, 2011 Big Sky, MT, United States. IEEE Computer Society.

EHRMANN, C. & HERDER, S. Integrated diagnostic and preload control for ball screw drives by means of self-sensing actuators. 2013 WGP Congress, July 22, 2013 - July 23, 2013, 2013 Erlangen, Germany. Trans Tech Publications Ltd, 271-277.

HEDBERG, T. & HELU, M. 2016. *Smart Manufacturing Systems (SMS) Test Bed* [Online]. Gaithersburg, MD: National Institute of Standards and Technology. Available: http://www.nist.gov/el/facilities_instruments/smstestbed.cfm [Accessed 2016].

HELU, M. & HEDBERG, T. 2015. Enabling smart manufacturing research and development using a product lifecycle test bed. *Procedia Manufacturing,* 1**,** 86-97.

HELU, M. & WEISS, B. A. The current state of sensing, health management, and control for small-to-medium-szed manufacturers. ASME 2016 Manufacturing Science and Engineering Conference, MSEC2016, 2016.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 2012. ISO 230-1 - Test code for machine tools – Part 1: Geometric accuracy of machines operating under no-load or quasi-static conditions.

JIN, X., SIEGEL, D., WEISS, B. A., GAMEL, E., WANG, W., LEE, J. & NI, J. 2016. The Present Status and Future Growth of Maintenance in US Manufacturing: Results from a Pilot Survey. *Manufacturing Review*.

KAGERMANN, H., HELBIG, J., HELLINGER, A. & WAHLSTER, W. 2013. *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry; final report of the Industrie 4.0 Working Group*, Forschungsunion.

KHAN, A. W. & CHEN, W. Calibration of CNC milling machine by direct method. 2008 International Conference on Optical Instruments and Technology: Optoelectronic Measurement Technology and Applications, November 16-19, 2008 2009 Beijing, China. SPIE, 716010.

LEE, J., GHAFFARI, M. & ELMELIGY, S. 2011. Self-maintenance and engineering immune systems: Towards smarter machines and manufacturing systems. *Annual Reviews in Control,* 35**,** 111-122.

LEE, J., NI, J., DJURDJANOVIC, D., QIU, H. & LIAO, H. 2006. Intelligent prognostics tools and e-maintenance. *Computers in industry,* 57**,** 476-489.

LIU, G. Control of robot manipulators with consideration of actuator performance degradation and failures. Robotics and Automation, 2001. Proceedings 2001 ICRA. IEEE International Conference on, 2001. IEEE, 2566-2571.

LY, C., TOM, K., BYINGTON, C. S., PATRICK, R. & VACHTSEVANOS, G. J. Fault diagnosis and failure prognosis for engineering systems: A global perspective. 2009 IEEE International Conference on Automation Science and Engineering, CASE 2009, 2009 Bangalore, India. IEEE Computer Society, 108-115.

MCKINSEY, G. I. 2012. Manufacturing the future: The next era of global growth and innovation. *McKinsey Global Institute*.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2015. *Measurement Science Roadmap for Prognostics and Health Management for Smart Manufacturing Systems* [Online]. Available: http://www.nist.gov/el/isd/upload/Measurement-Science-Roadmapping-Workshop-Final-Report.pdf [Accessed - 2016].

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2016. *Prognostics, Health Management, and Control (PHMC)* [Online]. Available: http://www.nist.gov/el/isd/ks/phmc.cfm [Accessed - 2016].

PCAST 2012. Report to the President: Capturing Domestic Competitive Advantage in Advanced Manufacturing. Executive Office of the President - President's Council of Advisors on Science and Technology.

SHIN, J.-H. & LEE, J.-J. Fault detection and robust fault recovery control for robot manipulators with actuator failures. Robotics and Automation, 1999. Proceedings. 1999 IEEE International Conference on, 1999. IEEE, 861-866.

TIAN, Z., LIN, D. & WU, B. 2012. Condition based maintenance optimization considering multiple objectives. *Journal of Intelligent Manufacturing,* 23**,** 333-340.

VOGL, G. W., DONMEZ, M. A. & ARCHENTI, A. 2016a. Diagnostics for geometric performance of machine tool linear axes. *CIRP Annals - Manufacturing Technology*.

VOGL, G. W., WEISS, B. A. & DONMEZ, M. A. 2015. A Sensor-based Method for Diagnostics of Machine Tool Linear Axes. *Annual Conference of the Prognostics and Health Management Society 2015.* Coronado, CA: PHM Society.

VOGL, G. W., WEISS, B. A. & HELU, M. 2016b. A review of diagnostic and prognostic capabilities and best practices for manufacturing. *Journal of Intelligent Manufacturing***,** 1-17.

WEISS, B. A., VOGL, G. W., HELU, M., QIAO, G., PELLEGRINO, J., JUSTINIANO, M. & RAGHUNATHAN, A. 2015. Measurement Science for Prognostics and Health Management for Smart Manufacturing Systems: Key Findings from a Roadmapping Workshop. *In:* SOCIETY, P. (ed.) *Annual Conference of the Prognostics and Health Management Society 2015.* Coronado, CA: PHM Society.

Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 00 (2016) 000–000

www.elsevier.com/locate/procedia

14th CIRP Conference on Computer Aided Tolerancing (CAT)

Towards Annotations and Product Definitions for Additive Manufacturing

Paul Witherell[a]*, Jennifer Herron[b], Gaurav Ameta[c]

"aNational Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899, USA"
[b]Action Engineering, 12081 W Alameda Pkwy, #455, Lakewood CO 80228, USA
[c]Washington State University, School of Mechanical and Materials Engineering, Pullman, WA 99164, USA

* Corresponding author. Tel: 1(301) 975-3385 ; *E-mail address:* paul.witherell@nist.gov

Abstract

As Additive Manufacturing (AM) is viewed more and more as a production-capable technology, data and information needs have made the costs of AM complexity increasingly apparent. Techniques available in current GD&T practices do not fully support product definitions needs in additive manufacturing. The fully model-driven process introduces new intricacies and complexities that must be addressed to facilitate the reproducibility of AM parts. Machine-readability needs must trump human interpretation requirements. In this paper, we discuss the future directions of GD&T and semantic annotations as they relate to satisfying AM product definition requirements.

© 2016 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the organizing committee of the 14th CIRP Conference on Computer Aided Tolerancing.

Keywords: Additive Manufacturing, Product Definition, PMI, GD&T

1. Introduction

As a true digitally-based process, Additive Manufacturing (AM) continues to shape our understanding of how a part is manufactured. While manufacturing processes have long been considered inhibitors of design freedoms, AM contests this perception, as noted with the phrase "complexity is free [1]." However, as AM is viewed more and more as a production-capable technology, the costs of complexity become increasingly apparent, albeit in a new form. Newfound design flexibilities are accompanied by the need to describe and communicate complex designs. In AM, due to the intricacies of the processes, the communication of design intent must often include process, or even material, specifics. For these reasons, AM is compelling us to rethink how we package and communicate design requirements.

As a stand-alone production process, AM requires a 3D model for a machine to execute its instructions. 2D drawings and traditional annotations lack the capacity to be machine-interpreted for an AM-destined part [2]. New methods are needed to support appropriate definitions and communicate full design-intent in AM. As an example, the locations of the temporary support structures often used in AM processes may be critical to the strength and functionality of the final part. This manufacturing "process" detail begins to blur the line between design requirements and manufacturing plans, redefining how the mechanical hardware industry has typically provided design trait definition.

Geometric Dimensioning and Tolerancing (GD&T) practices are widely established as a means for conveying design intent for manufacture and inspection. However, until recently, GD&T practices have mostly been rooted in two-dimensional space. With the rise of Model-Based Engineering (MBE), the benefits of 3D product definition become increasingly apparent yet slow to evolve. AM has the potential to not only expedite, but also shape this evolution, as Model-Based Definition (MBD), a technique of communicating a product using the 3D model geometry and 3D annotations, is ideally suited for parts and assemblies built with AM methods.

A distinction critical to the conversation surrounding MBD methods is to understand the difference between annotations that are intended for human consumption (through presentation) versus those that are intended for computer

2212-8271 © 2016 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the organizing committee of the 14th CIRP Conference on Computer Aided Tolerancing.

consumption (through representation). Annotations (dimensions, notes, geometric tolerances, etc.) that are human destined are *presented* graphically. Annotations that are computer destined can be *represented* as data structures that can be interpreted by software. Elements of representation (or semantic) annotations are cautiously being introduced into GD&T practices through the ASME Y14 series committees[1] and ISO TC 213 committees[2]. To satisfy design definition for AM, these MBD elements must be both satisfied *and* extended. In this paper, we discuss annotation challenges created by AM, and the future of 3D product definitions and semantic annotations as they relate to overcoming these challenges.

2. Background

With traditional, subtractive manufacturing processes, the specifications provided by the GD&T community sufficiently support the verification and validation of manufactured parts. However, these same practices are insufficient for providing the unambiguous definitions necessary to guide how an AM part is manufactured and inspected. In [2], suggestions were made for how available techniques could be adapted to meet both the geometry and process-specific needs of AM. Comparisons were made on how AM needs compare with those seen in castings, forgings, and composites (Table 1). As the table indicates, several AM challenges are implementable using adaptations of available techniques; however, the question of practicality soon arises. A proper solution requires extending product definition to accommodate AM practices.

Table 1: Summary of parameters and tolerances described in ASME Y14.8 standard on castings, forgings and moldings [3]and ISO/DIS 8062-4 [4]that could be adapted and applied to AM. Table derived from [2].

Existing Technique	AM Counterpart
Cast, Forged, Mold part related requirements	
Parting line/plane	Build Plate
Mold line	Build Plate
Forging plane	Build Location
Grain direction	Build Direction
Grain flow	Inspection
Draft angle and tolerance	Build Direction
Die closure tolerance	Support Structures
All around and all over tolerances on different sides of parting plane	All around and all over tolerances
Required machining allowances	Post-processing allowances
Composite part related requirements	
Ply	Layer
Ply orientation	Scan Pattern
Ply Table	Scan Pattern by Layer

Similar to what has been encountered with castings, forgings, and composites [3, 5], how AM parts are processed will significantly impact whether or not the part is able to meet functional requirements. With AM processes, consistency in production is challenged by many possible variants. As a result, additional information related to AM processes may have to be conveyed by the designer at design time. In [2], AM challenges with process specifics such as build directions, support structures, and hatch plans were raised (Table 1). To achieve "as designed" functionality, "as processed" declarations must be made. If AM is to be treated as "just another process," design requirements must hold and designers must have the ability to fully communicate process specifics.

As AM continues to emerge as a viable industry technology for the production of functional parts and assemblies, an accompanying need has emerged to ensure reproducibility in AM part design and functionality. As a purely model-driven manufacturing process, the role of drawings in the lifecycle of a product created with AM diminishes and, in many use cases, begins to have very little value. It is critical that the 3D model become the master data definition for a product produced with AM. Current GD&T annotation practices must evolve to a point where they are embedded within the modeling environment, allowing for "clickable" symbolics, and perhaps more importantly, semantic product definitions.

With Computer-aided technologies (CAx) and systems becoming, if not already, commonplace in industry, digital representations are increasingly used to supplement (and sometimes replace) drawings as a mechanism for communicating part geometry and specifications [6]. CAx systems provide a digital backbone on which information can be structured and stored. Accordingly, in what can be described as a transition to digital manufacturing, MBE requires users to create digital packages that can be interpreted by humans and computers[7, 8]. These digital packages are beginning to incorporate Product and Manufacturing Information (PMI), or annotations on a CAD model to precisely define product geometry and product specifications [8]. However, where product definition needs in traditional manufacturing can be satisfied by available annotation methods, including presentation methods, AM product definitions cannot.

3. Product Definitions: Transitioning from GD&T to PMI

In the traditional sense, GD&T is exactly as it states, a means for specifying dimensions on geometry and communicating allowable dimensional and geometric variations (tolerances) for which manufacturing can be planned and inspections can be made. Parts with tight tolerances may require precision machining methods, while loose tolerances may allow for greater flexibility. In the past, basic drawing annotations have been successful in telling manufactures how the final part should appear, entrusting the manufacturer with many, if not most of the process details to arrive at a desired state. Drawings and annotations have effectively enabled product end-users to validate their part against a design, ensuring that the part they were in possession of was indeed the part they were intended to have.

As designers learn to take advantage of the unique design opportunities provided by AM, they must also learn to plan and account how processing may affect their design intent. As some look to treat AM as "just another" manufacturing process [9-11], this is not be the case when communicating specific design requirements. When considering AM challenges, we must consider GD&T in the context of the service it provides, a means for the designer to communicate design requirements from the design through the manufacture to the part inspection (Figure 1).

[1] https://cstools.asme.org/csconnect/CommitteePages.cfm?Committee=C64000000

[2] http://www.din.de/en/getting-involved/standards-committees/natg/international-committees/wdc-grem:din21:83875112

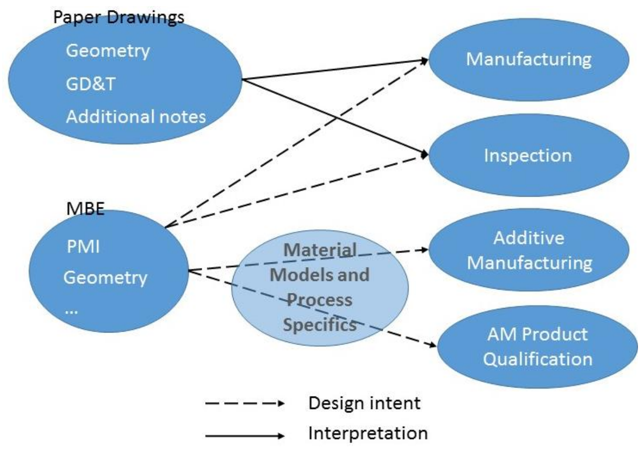


Fig. 1: MBE based communication has design intent embedded, mitigating misinterpretations.

It is crucial to avoid blindly transitioning 2D methods onto a 3D model, because the mathematical models and assumptions are different, and to take advantage of opportunities to improve any inefficiencies that exist with 2D drawing methods. The literal definition of GD&T falls short in meeting and communicating the design requirements from design through to part inspection for AM. In [12], the authors explore the role of traditional engineering drawings versus model-based definitions. They note that MBDs offer additional functionalities that can actively and proactively control product data.

In MBE practices, product definitions [13] have become the standard means for communicating requirements. With AM products, comprehensive product definitions are needed to facilitate (a) clarity in the communication, (b) efficiency in the as-built versus as-designed comparison, and (c) increased product quality. It is with these considerations that we discuss the need to transition from GD&T to PMI. Efforts to create a product definition in AM must support repeatability in a process in attempt to achieve reproducibility in parts. GD&T challenges with respect to AM will be discussed based on complex geometries, material-process interactions and internal features.

3.1 Complex geometries

Challenges in communicating AM design intent begin with complex geometries. In [2] the authors discuss geometries that are not necessarily specific to additive manufacturing, but are highlighted because of AM’s unique capabilities. Many of these geometry types are currently unsupported by GD&T practices, and would be very difficult, if not impossible, to communicate through direct adaptations of these practices. Additionally, complex surfaces, created by methods such as topological optimization, may require numerous tolerance annotations at various locations. Such numerous tolerance annotations lead to ambiguity, hampering the purpose of GD&T. Therefore new methods of tolerancing complex surfaces may be required to address the presentation and representation of tolerancing requirements.

In the case of topological optimization, geometry is determined by the functional requirements of the part, so inconsistencies in geometry may directly relate to part failure. The top part in Figure 2, a hand structure, is an example of a freeform geometry where the shapes and surfaces may have specific functional implications. Note that that the provided annotations are insufficient for communicating tolerances on the geometry shown, as they correlate with only partial features of a very complex shape. The lower part demonstrated in Figure 2 was created to meet required strength and have minimum weight that can be produced using AM technology. The communication of allowable variations in these intricate geometries is not feasible through available GD&T techniques. Only the traditional surfaces can be toleranced using GD&T. Freeform surfaces with varying thickness or tolerances cannot be toleranced.

3.2 Material – process interaction

One of the most unique, and consequential, considerations that must be addressed in AM product definitions is how to account for material and process interactions. Though AM material specifications are in development[3], they are proving themselves to be highly dependent on process parameters (Most machine manufacturers will provide their own materials to be processed by predetermined and pre-set parameter sets to

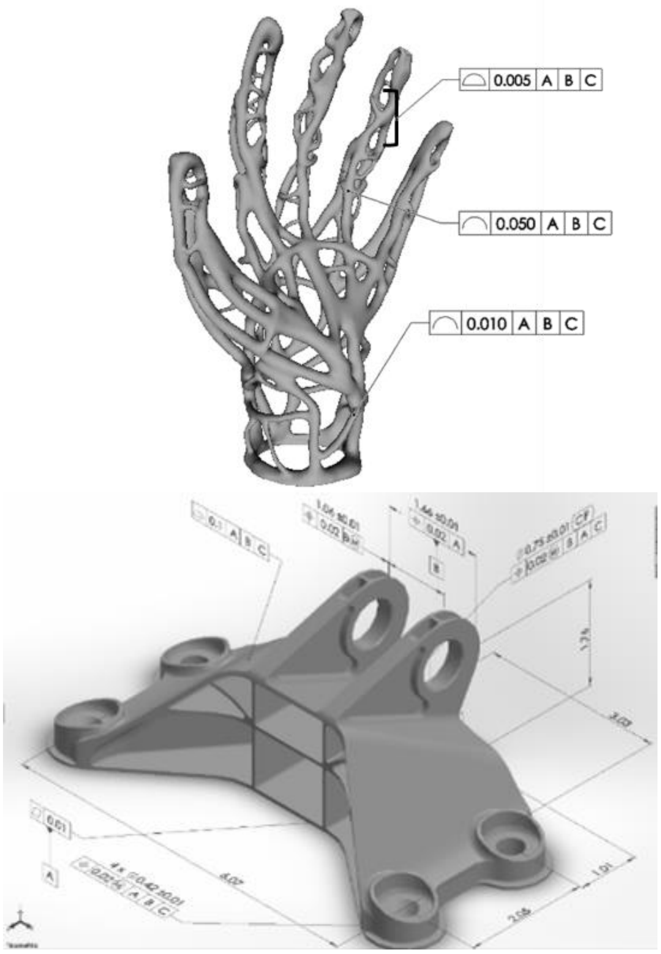


Fig. 2: Top: Example of applied tolerances on freeform geometry such as an organic structure[4]. Line and Surface profiles are allocated to demonstrate complexity. Bottom: Modified version of the topology optimized part from the GE bracket design competition [20] winner [21] with GD&T.

[3] http://www.astm.org/COMMIT/SUBCOMMIT/F4205, https://www.sae.org/works/committeeHome.do?comtID=TEAAMSAM

[4] Figure is derived from a model of a branched hand found on Makerbot Thingiverse (http://www.thingiverse.com/thing:332451)

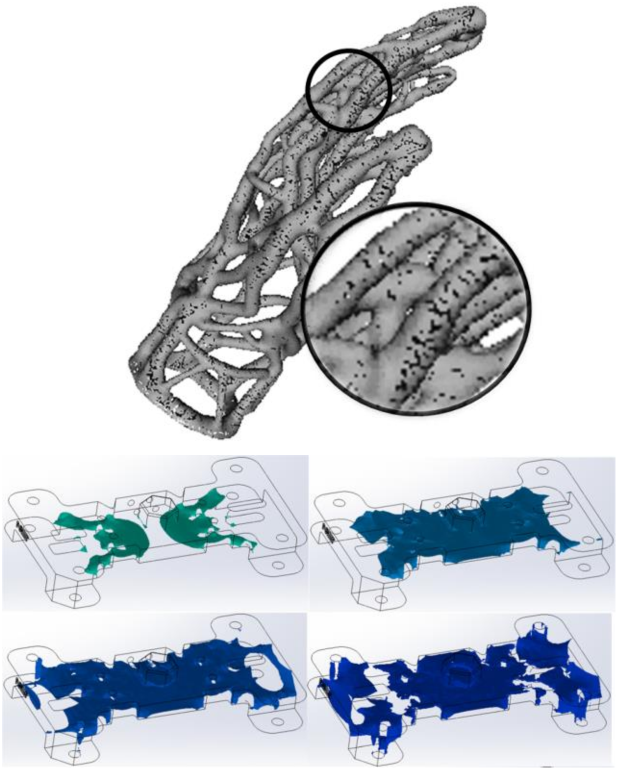


Fig. 3: Top: Example where voids may be engineered into a part to provide specific functionality. Bottom: Graded material distribution shown as surfaces and volumes in a part[5]. Various materials and processes metrics would be needed in order to semantically communicate this information.

mitigate material-process variability). AM, even more so than composites, is a process where the characteristics of the part cannot be determined until after the process is completed and the geometry has been formed. For this reason, how the material is processed must be accounted for in the product definition.

As AM technology matures, process communication challenges for a designer will be further compounded when engineering multi-material functionality into a design. AM is also unique in that part mechanics and performance can be digitally manufactured using multiple materials. Functionally graded materials are seen by many as a major breakthrough made possible by AM processes, and combine process and geometry characteristics.

When functional grades are designed into a part, to manufacture these grades metrics must be communicated about specific material locations in relation to process specifics (Figure 3). These multi-material parts epitomize the challenges AM can create with material processing. Testing for functionality will also create challenges, and additional information would have to be communicated about inspection as well (e.g., to communicate location-specific performance specifications). This again extends far beyond what is currently understood as GD&T. In [12], the authors conclude that the great majority of the MBD benefits will potentially be captured at the manufacturing and inspection levels, which happen to be the greatest areas of need in AM processing environments.

3.3 Internal Features

A unique trait of AM part production is the ability to create internal features that are not possible with other manufacturing methods. As such, specific inspection techniques may be required to ensure that the final parts meet design specifications. Non-Destructive Testing (NDT) is becoming an increasingly important instrument in qualifying parts against AM designs. Such methods are often necessary for measuring internal features or cavities without causing damage to a part. They also provide a means for studying potential variations between processed layers. For these reasons, it is conceivable that the designer may want to communicate to the inspector not only what needs to be measured within the part, but also what technique to use to measure it, and what acceptable tolerances are.

To treat AM as simply "another manufacturing process," we must rethink how we communicate, interpret, and act upon information related to product definitions. Specifically, we must look past traditional GD&T annotations and explore what PMI and product definitions must convey in order to satisfy AM needs. To incorporate AM into production lines as an "alternative manufacturing process," a large amount of additional geometry information, manufacturing information, and inspection information may need to be included in any data package associated with the part.

Until now, the discussion has focused on extending GD&T information as part of a larger set of PMI, why this extension of data is necessary in AM, and what some of this data may look like. What we have not discussed is the *how*, or how current practices can support the communication of this potentially vast amount of information. In the next section, we investigate the role semantics may play in communicating product definitions to support future AM MBE needs.

4. Product Definitions: Transitioning from Symbols to Semantics

As manufacturing has become an increasingly digital process, GD&T as a symbolic language for communication continues to be pressed. It is a common GD&T practice to require that all dimensions must have a tolerance [14]. With traditional GD&T and symbology, annotations are attached through notations. The number of dimensions necessary to define complex, organic shapes on a 2D drawing can quickly multiply, and in some cases are time limiting to create. Many organizations have turned to 3D model geometry as the master of the geometry, a tenet of MBD. However, a true transition from traditional GD&T practices to a 3D product definition (using appropriate PMI schemes) requires more than a superficial makeover. The fundamentals must be addressed as well.

From purely a GD&T standpoint, symbolic definitions are important to the human reader, to be able to comprehend the design, manufacturing or inspection intent, but are not necessarily ideal for computer consumption. A transition from human readable only symbolism to a greater reliance on semantics is a necessary step to bring AM nearer to full MBE [15] [16]. The differences between symbolism and semantics are recognisable when considering how PMI is communicated through presentation and representation, where:

[5] http://www.nist.gov/el/msid/infotest/mbe-pmi-validation.cfm

Presentation (Graphic Annotation) is intended for visual consumption and human readability only (Figure 4), and[6]

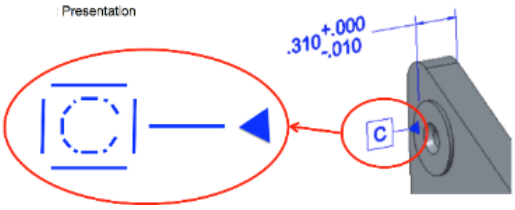


Fig. 4: Example depicting the concepts of presentation.

Representation (Semantic Annotation) is intended for software consumption. Data elements are encoded in the 3D digital model and associated to their product features and may also be human readable (Figure 5).[5]

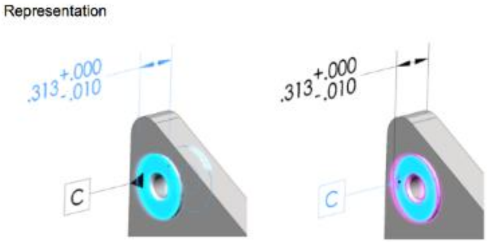


Fig. 5: Example depicting the concept of semantic annotations that represent digitally associated annotations.

Current practices using models and product definitions can be grouped into two categories: Model plus Drawing or Model-Only [17]. Using only 2D drawing graphics sheets and symbolic presentation to communicate an AM product into the CAM software required to drive the AM machine is inadequate, as AM processes are inherently model-driven. Therefore, Model-only product definitions are required for AM. These product definitions allow annotated 3D geometry to move from CAD (Computer-Aided Design) software into CAM (Computer-Aided Manufacturing) software without the need for a drawing or drawing graphics sheet [18].

Desired applications for AM include:

- Semantics to manage process-specifics across platforms while still maintaining the ability to communicate information so it can be interpreted reasonably
- Semantics to supplement visual aids/ semantics to guide visual interpretations based on interest (symbolic/semantic hybrid)
- Semantics to support automated inspection

A transition to representative, semantic annotations, attributes and metadata would not only reduce the amount of visual communication needed, but could also be used to template methods for communicating complex geometries and additional PMI.

The amount of information potentially communicated for an AM part also creates challenges specific to tolerancing methods, challenges that may be best addressed with semantic approaches. In discussing tolerancing with traditional GD&T methods, Wang notes that “tolerancing semantics such as logical dependency among variations and sequence of specifications is not maintained in these models” [19] [20]. Given the layer-by-layer nature of AM processes, it is immediately apparent that sequential tolerancing may be needed. Wang maintains a semantic tolerance modeling scheme based on general intervals is needed to improve interoperability of tolerance modeling. The author notes, “With the theoretical support of semantic tolerance modeling, a new dimension and tolerance specification scheme for semantic tolerancing is also proposed to better capture design intents and manufacturing implications, including flexible material selection, rigidity of specifications and constraints, component sorting in selective assembly, and assembly sequences.” This list of benefits aligns well with complexities introduced by AM.

Beyond the layer-by-layer sequences, it is likely that distinguishing between several intermediate stages will be necessary to communicate different AM part requirements. For example, if trying to avoid process specifics, the argument may be made that support structures do not need to be addressed in the product definition. As noted in Section 2, however, process specifics such as the placement of support structures can directly influence both the shape and function of a part. In Selective Laser Melting (SLM) processes, for instance, support structures act as a heat sink during processing, relieving thermal stresses that are created during the build. These thermal stresses can create warping if not properly relieved. For this reason, the locations of support structures can greatly influence the quality of a build.

Accommodating for intermediate stages [21] (Figure 6) can create significant challenges when using symbolism to communicate product definition, especially in terms of presentation and consumption. Semantics can appropriately address such challenges by communicating through machine interpretable data calls as opposed to tables and graphs. In short, given the typically complex geometry of AM, in conjunction with the requirements of AM processing, it is imperative that new methods be developed for defining the “complete” AM product.

5. Product Definitions: Next Steps

As noted in Sections 3 and 4, AM pushes current GD&T practices to their limits, and, as the technology matures, these limits will be far exceeded. As AM technology matures, designers may look to intentionally engineer porosity into designs (Top, Figure 3), changing how a part may respond to particular loading conditions. Current design for AM is often restricted to a single material, though multiple material options are emerging, as noted in Section 3. As designers learn to introduce heterogeneity into part performance, the need to bridge design and process communication becomes increasingly important.

A finished AM part may be observed as two stages, one stage after the AM processing is completed, and one stage after the post processing is completed. New machines are now integrating these stages, where the build and the post processing are occurring in concert as a hybrid AM process. While this simplifies the process, it also highlights the necessities of machine-interpretable PMI (annotations, attributes and metadata). Hybrid machines would be enabled to process differences, where otherwise manual adjustments may have to be made.

[6] Action Engineering, Re-Use Your CAD MBE Workshop, http://www.action-engineering.com/pdf/CIC-2012_MBEWorkshop.pdf

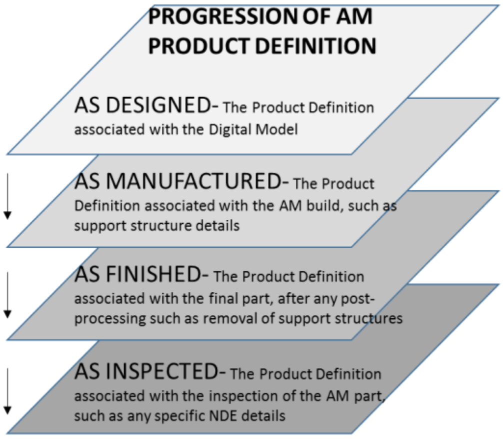

PROGRESSION OF AM PRODUCT DEFINITION
AS DESIGNED- The Product Definition associated with the Digital Model
AS MANUFACTURED- The Product Definition associated with the AM build, such as support structure details
AS FINISHED- The Product Definition associated with the final part, after any post-processing such as removal of support structures
AS INSPECTED- The Product Definition associated with the inspection of the AM part, such as any specific NDE details

Fig. 6: Intermediate stages of AM product definition.

Also noted in Section 4 (and Figure 6) are the inspection challenges that AM may create. Internal features can not be readily inspected via traditional inspection CMM (Coordinate Measuring Machines). Additional non-destructive scanning technologies such as Computerized Axial Tomography (CAT) scans may be required to validate internal geometry. Still in their infancy (both in definition and technology to implement), automated 3D inspection capabilities have the potential to completely change the landscape of a "quality" product. Once we have design intent captured in semantic (digitally associated software readable) annotations, attributes and metadata, then the next steps of automated inspection can take place.

In summary, the challenges associated with communicating GD&T in AM are just beginning to emerge. As the technology matures, new methods will be necessary to communicate design intent, and these methods must rely heavily on PMI and representation techniques. The next steps necessary for support of AM product definitions include:

1) Developing methods to tolerance complex, freeform surfaces not currently supported,
2) Developing methods to communicate and tolerance heterogeneous materials and internal geometries,
3) Developing methods to communicate dimensioning and tolerancing requirements at multiple stages of a single product lifecycle,
4) Developing methods to facilitate machine-readable dimensioning and tolerancing from design to manufacture to conformance and verification.

Each of these conditions extend beyond current GD&T capabilities, yet must be satisfied to meet AM product definition requirements. As MBE continues to develop, current GD&T practices have been able to keep pace. To achieve the reproducibility required by a production alternative, an unprecedented amount of design information must be communicated for an AM product. To effectively meet these needs, AM, will *require* us to adapt what we currently understand to be GD&T and embrace the underlying principles of both PMI and semantic content. This thinking will change the landscape of manufacturing.

Acknowledgements

The authors are grateful to Joshua Lubell for his helpful and insightful comments on an earlier draft of this paper. Any remaining mistakes are the authors' sole responsibility.

Disclaimer

Certain commercial equipment, instruments, or materials are identified in this paper. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

References

[1] Friedman, T.L., (2013): When Complexity Is Free, in: The New York Times NY, NY, September 14, 2013.
[2] Ameta, G., Lipman, R., Moylan, S., Witherell, P.,(2015): Investigating the Role of Geometric Dimensioning and Tolerancing in Additive Manufacturing, J Mech Design, 137 111401.
[3] ASME, (2009): ASME Y14.8 Casting, Forgings and Molded Parts, in, ASME, New York.
[4] ISO/ DIS, (2015): Geometrical product specifications (GPS) -- Dimensional and geometrical tolerances for moulded parts -- Part 4: General tolerances for castings using profile tolerancing in a general datum system, in, ISO/DIS.
[5] ASME, (2012): Y14.37: Composite Part Drawings, in, ASME, New York.
[6] Jackson, C., (2014): The State of Model Based Enterprise Report, in: L. Insights (Ed.).
[7] Feeney, A.B., Frechette, S.P., Srinivasan, V.,(2015): A portrait of an ISO STEP tolerancing standard as an enabler of smart manufacturing systems, Journal of Computing and Information Science in Engineering, 15 021001.
[8] Lipman, R., Lubell, J.,(2015): Conformance checking of PMI representation in CAD model STEP data exchange files, Computer-Aided Design, 66 14-23.
[9] Fuges, C.M., (2014): Multiplying Options, in: Additive Manufacturing.
[10] Ayers, K.L., (2014): SME Speaks: From a Miracle to Just Another Tool, in: Manufacturing Engineering.
[11] Bastian, A., (2015): Understanding The 3D Printing Ecosystem, in, Techcrunch.
[12] Quintana, V., Rivest, L., Pellerin, R., Venne, F., Kheddouci, F.,(2010): Will Model-based Definition replace engineering drawings throughout the product lifecycle? A global perspective from aerospace industry, Computers in Industry, 61 497-508.
[13] ASME, (2012): ASME Y14.41 Digital Product Definition Data Practices, in, ASME, New York.
[14] Kim, N.-H., Kumar, A., Snider, H.F., (2014): Geometry of design: A workbook, Elsevier.
[15] Lubell, J., Chen, K., Horst, J., Frechette, S., Huang, P.,(2012): Model based enterprise/technical data package summit report, National Institute of Standards and Technology. US Department of CommerceSpringer Berlin Heidelberg.
[16] Sarigecili, M.I., Roy, U., Rachuri, S.,(2014): Interpreting the semantics of GD&T specifications of a product for tolerance analysis, Computer-Aided Design, 47 72-84.
[17] Herron, J., (2013): Re-Use Your CAD: The Model-Based CAD Handbook, CreateSpace Independent Publishing Platform.
[18] ASME, (2012): ASME Y14.1 Decimal Inch Drawing Sheet Size and Format in, ASME, New York.
[19] Wang, Y.,(2007): Semantic tolerancing with generalized intervals, Computer-Aided Design and Applications, 4 257-266.
[20] Wang, Y., (2006): Semantic tolerance modeling–An overview, in: Proc. Industrial Engineering Research Conference (IERC'06), Citeseer.
[21] Kim, D.B., Witherell, P., Lipman, R., Feng, S.C.,(2015): Streamlining the additive manufacturing digital spectrum: A systems approach, Additive Manufacturing, 5 20-30.

Quantized Hall resistance in large-scale monolayer graphene

Yanfei Yang[1], Chiashain Chuang[1,2], Chieh-Wen Liu[1,3] and Randolph E. Elmquist[1]

[1] National Institute of Standards and Technology, Gaithersburg MD, 20899 USA; [2] Depart of Physics, National Taiwan University, Taipei 106, Taiwan; [3] Graduate Institute of Applied Physics, National Taiwan University, Taipei 106, Taiwan

E-mail: Elmquist@nist.gov

Abstract: **Graphene is a one-atom-thick carbon lattice that can be exfoliated from solid graphite or grown using high temperature processing methods on a variety of substrates. Many practical applications of large-area graphene, however, are limited by the transport mobility and carrier concentration homogeneity over distances greater than hundreds of microns. This presentation reports on the characteristics of large area (5 mm^2 to 25 mm^2) monolayer devices that display precise quantum Hall effect (QHE) characteristics at reasonable cryogenic temperatures, surpassing the previously reported records for graphene.**

Keywords: quantum Hall effect, graphene, electronic mobility, resistance standard

1. INTRODUCTION

Epitaxial graphene (EG) [1,2] is formed when silicon (Si) sublimates at high temperature on the surface of SiC(0001), a hexagonal crystalline material with a wide band gap. [3] The EG samples grown in our laboratory are annealed facing a glassy graphite disk. The role of vapor-phase byproducts (Si, Si$_2$C and SiC$_2$) is increased due to the geometrical arrangement of the substrate and confining graphite surface. [4] The result is a uniform EG monolayer over a large area, while bilayer graphene is suppressed and sometimes absent at millimeter scale.

We find that face-to-graphite (FTG) growth [5] in Ar background gas halts at one monolayer over most of the surface at temperatures up to 2000 °C. The optical images in figure 1(a,b) show two samples processed concurrently at 1950 °C (1800 s). Note that only ≈ 100 µm of the surface near the edge of the FTG sample (figure 1a) has dark graphite filling the etched pits, while the interior region of the FTG sample is much more uniform. This uniform appearance is in contrast to the sample processed open to Ar background gas (figure 1b), which has a disordered EG layer and dark graphite covering all of the pits. Raman microscopy, optical

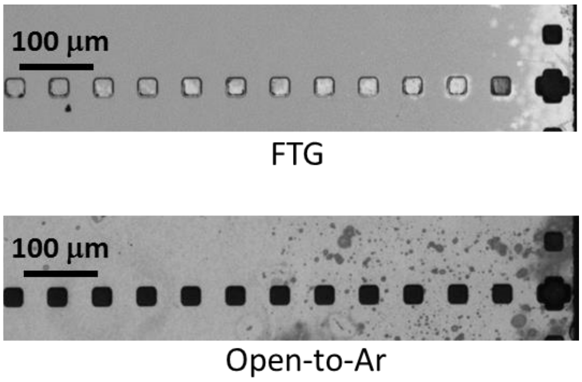


Figure 1. Optical microscope images showing the difference in EG near border regions of two samples processed together, (a) FTG and (b) open to Ar gas in the furnace.

SP-1087

Yang, Yanfei; Chuang, Chiashain; Liu, Chieh; Elmquist, Randolph.
"Quantized Hall resistance in large-scale olayer graphene."
Paper presented at the Brazilian Congress on Metrology: 2015, Bento Gonçalves, Brazil, Nov 29-Dec 4, 2015.

images, atomic force microscopy (AFM), and electronic transport characteristics all show that the interior of FTG samples consists of uniform monolayer EG without appreciable inclusion of bilayer patches and with small atomic step heights.

2. FABRICATION AND SELECTION

Optically enhanced (OE) microscope imaging [6] makes visible the small (≈ 2.3 %) difference in transmission that occurs for light passing through a single layer of graphene, compared to the transmission through the insulating SiC substrate from which the EG has been removed. Figure 2 shows one large device that was processed at 1900 °C (116 s), fabricated using a low-residue technique with a sacrificial 20 nm protective Pd/Au layer [7], photographed using OE microscopy, and measured using low-frequency ac magneto-transport. The images in the lower part of figure 2 show six regions of the sample near the Hall bar device with uniform OE contrast indicating homogeneous EG coverage. The two sets of magneto-transport characteristics shown in the upper part of figure 2 also indicate that the EG is monolayer graphene, with uniform carrier concentration n. The values of resistivity $\rho_{xx} = (R_{\mathrm{A}xx}/2 + R_{\mathrm{B}xx}/2) \times w/L$ were derived from the average resistance along both sides of the device and scaled by the ratio of width to length separating the potential terminals at the ends of region 1 and region 2.

Both regions of the device shown in figure 2 display similar transport characteristics with $R_{xy} \approx 12906.4\ \Omega$ for magnetic field $B > 5$ T at temperature $T = 1.5$ K. In the OE images, the main visible features are the SiC atomic terrace edges which appear as darker diagonal lines, and form at high temperature as the EG layer grows. Large terraces can be formed with atomic steps of height up to 10 nm, and these steps reduce the mobility by increasing the electronic scattering in EG [8]. We have found that for fixed carrier concentration n the mobility $\mu = \rho_{xx}(B{=}0)/ne$ is improved by reducing the height of extended terraces to $h < 3$ nm. As the OE images of figure 2 scan progressively from left to right and are seen to be longer and more distinct, AFM shows that they increase in height. This coincides with

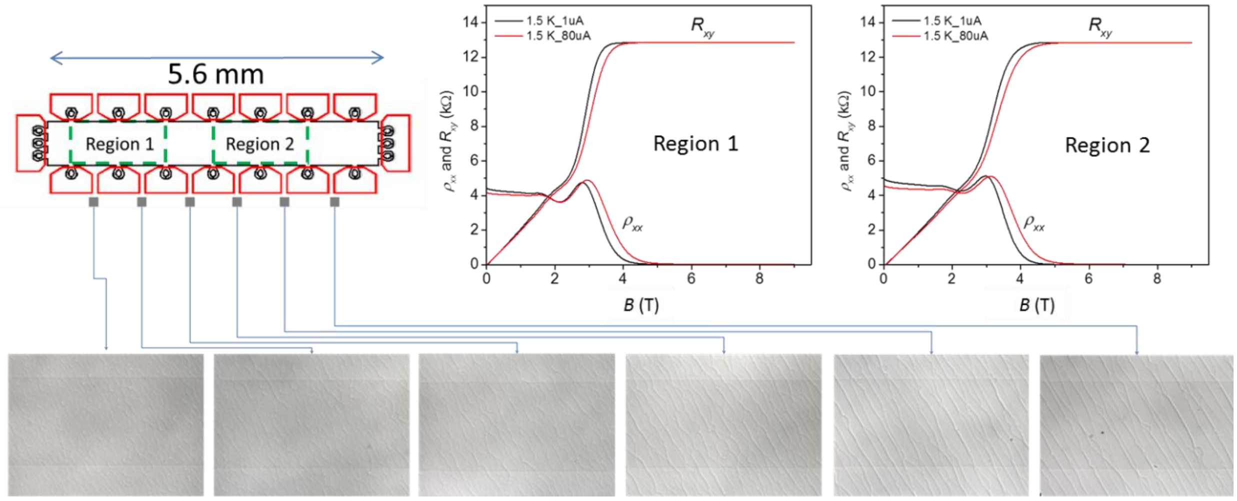


Figure 2. Design, magneto-transport characteristics, and OE images of a 5.6 mm long Hall bar device. The Hall bar channel is surrounded by multiple contacts so that the characteristics of different regions can be measured. Both region 1 and region 2 display excellent QHE plateaus, but the mobility of region 1 is 20 % higher as described in the text. This improvement corresponds to low and irregular terraces in the OE images at bottom, where EG is bordered at top and bottom by bare SiC.

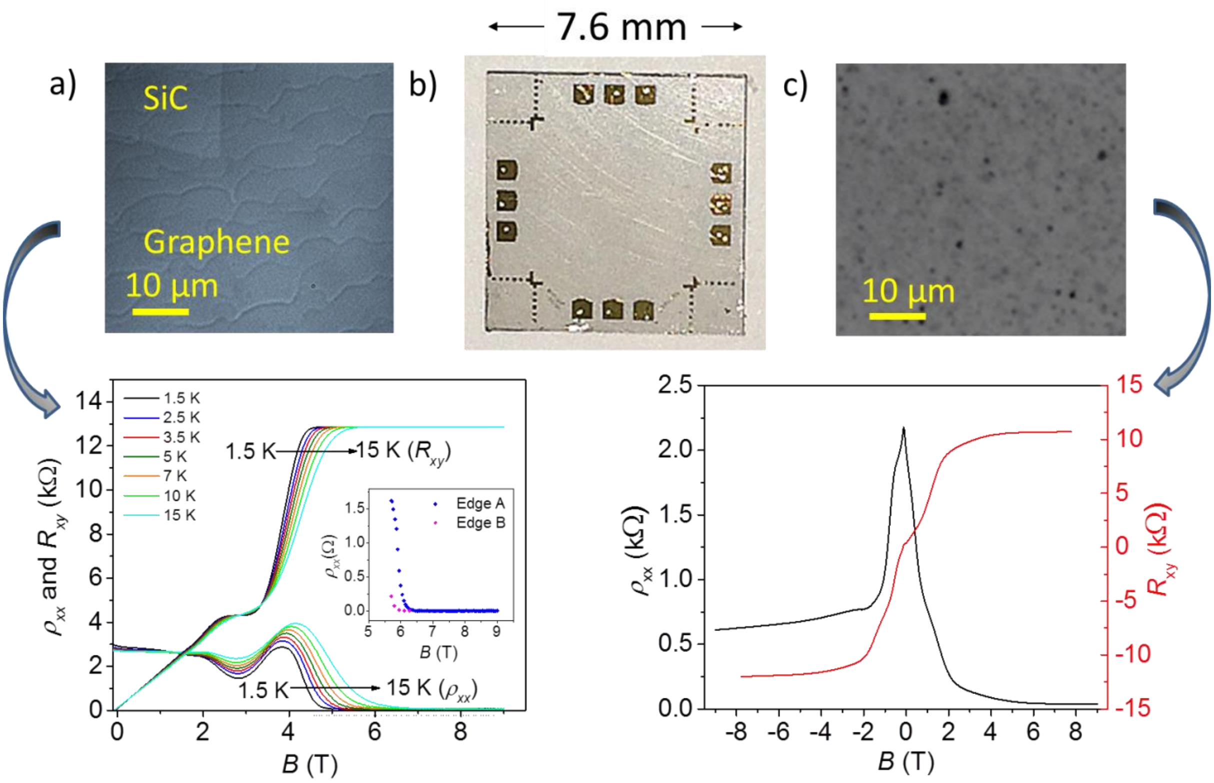


Figure 3. Large octagonal devices. The device shown in (a) and (b) was produced from FTG graphene, while the sample shown in (c) was annealed open to argon background gas. The QHE plateau is robust up to at least 15 K in the FTG sample, with full quantization above 7 T as shown in the inset. Only very weak QHE plateaus are observed for the sample in (c), with non-symmetric longitudinal resistivity for ±*B*.

the reduction in mobility from 4600 cm^{2}V^{-1}s^{-1} in region 1, to 3840 cm^{2}V^{-1}s^{-1} in region 2.

3. CHARATERIZATION

A robust quantum Hall effect has been observed in devices of octagonal shape as well as in the Hall bar configuration. Large octagonal samples were produced using both FTG and open-to-Ar graphene on SiC substrates. The FTG process clearly results in improved QHE properties in large samples when the EG is grown at 1900 °C, as shown in figure 3. Figure 3a shows an OE image and gives the Hall resistance R_{xy} and longitudinal resistivity ρ_{xx} for one such large, octagonal device of size 5.6 mm × 5.6 mm. This device shows resistance plateaus for the Landau-level filling factors $\nu = 6$ and $\nu = 2$ above about $B \approx$ 2.5 T and 6 T, respectively, indicating a moderate level of carrier concentration ($n \approx 4 \times 10^{11}$ cm^{-2}), which is sufficient for the QHE $\nu = 2$ plateau to be fully quantized. The device mobility is relatively high (5600 cm^{2}V^{-1}s^{-1}), owing to the low terrace steps and high-quality monolayer EG.

The $\nu = 2$ QHE plateau of this device is well quantized between 7 T and 9 T, with longitudinal resistivity ρ_{xx} = -150 μΩ ± 250 μΩ (σ = 1), or $\rho_{xx} < 10^{-8} \times R_{xy}$ with dc source-drain currents I_{SD} = ±74 μA and T = 2.6 K. Because the wide sample geometry limits the resolution at low currents, ρ_{xx} data was obtained using a precise nanovoltmeter and measurements of R_{xy} were made with a cryogenic current comparator bridge [9, 10]. We will report these results as well as other precise QHE measurements showing that EG devices are suitable as quantized Hall resistance standards, and possibly superior to most GaAs heterostructures now in use as resistance standards at many national laboratories.

4. DISCUSSION

Our results confirm and expand on many prior experiments showing that annealing SiC(0001) in confined Si vapor allows controllable EG growth. For the standards community, traceability from the QHE standard to 1 kΩ and 10 kΩ at current levels greater than 0.5 mA is within the capabilities of present-day room-temperature commercial resistance bridges, with relative uncertainty approaching 1 × 10^{-8}. Our results show promise for EG in studies of the frequency- and size-dependent electronic properties of graphene. Wafer-scale low-defect graphene also may lead to large-scale optical applications, high-frequency integrated circuits, optoelectronics and other useful applications.

5. REFERENCES

[1] Ruan M, Hu Y, Guo Z, Dong R, Palmer J, Hankinson J, Berger C and de Heer W, 2012 *MRS Bulletin* **37** 1138

[2] Forti S and Starke U 2014 *J. Phys. D: Appl. Phys.* **47** 094013

[3] Borovikov V and Zangwill A 2009 *Phys. Rev. B* **79** 245413

[4] Real M, Lass E, Liu F, Shen T, Jones G, Soons J, Newell D, Davydov A and Elmquist R 2013 *IEEE Trans. Instrum. Meas.* **62** 1454

[5] Camara N, Huntzinger J, Rius G, Tiberj A, Mestres N, Pérez-Murano F, Godignon P and Camassel J 2009 *Phys. Rev. B* **80** 125410

[6] Yager T, et al. 2013 *Nano Lett.* **13** 4217

[7] Yang Y. Huang L, Fukuyama Y, Liu F, Real M, Barbara P, Liang C, Newell D and Elmquist R 2015 *Small* **11** 90

[8] Ji S, Hannon J, Tromp R, Perebeinos V, Tersoff J and Ross F 2012 *Nature Mat*. **11** 114

[9] Bierzychudek M and Elmquist R 2009 *IEEE Trans. Instrum. Meas*. **58** 1170

[10] Hernandez-Marquez F, Bierzychudek M, Jones G and Elmquist R 2014 *Rev. Sci. Instrum.* **85** 044701

Yang, Yanfei; Chuang, Chiashain; Liu, Chieh; Elmquist, Randolph.
"Quantized Hall resistance in large-scale olayer graphene."
Paper presented at the Brazilian Congress on Metrology: 2015, Bento Gonçalves, Brazil, Nov 29-Dec 4, 2015.

SP-1090

High-temperature Material Constitutive Models for Structural-Fire Analysis

CHAO ZHANG, LISA CHOE and JOHN GROSS

ABSTRACT

The applicability of three steel constitutive models was evaluated using finite-element analyses and various member capacity equations. Three different high-temperature stress-strain models were compared: the model recently developed by the National Institute of Standards and Technology (NIST) [1], the Eurocode 3 model [2] and the model developed by Lie [3]. The testbed used in the analyses included twenty steel column tests and two restrained steel beam tests reported in the technical literature. The selected column tests reported buckling temperatures ranging from 500 ^{o}C to 700 ^{o}C and applied axial load ranging from 20 % to 65 % of the axial-load capacity at ambient temperature. Each reported test was analyzed in two different ways: (1) finite-element model was developed to predict the buckling temperature of the steel columns and response of the restrained steel beams in fire condition. (2) member capacity equations prescribed in Eurocode 3 and ANSI/AISC-360-10 [4] were used to compute the buckling temperature of the steel columns. Overall, the results indicate that all investigated material models give acceptable prediction of the buckling temperature of the steel columns and the behavior of restrained beams. The finite-element model with the NIST and the Lie material models predict the buckling temperature more accurately than that with the EC 3 material model. When the Eurocode column capacity equations were used, the buckling temperatures calculated using the NIST and the EC 3 models are more comparable with test results than those using the Lie model. It was also found that the current ANSI/AISC 360-10 Appendix 4 equation conservatively estimate the buckling temperature of the tested column specimens with difference of 20% on average. When the standard column equation in the Chapter E of ANSI/AISC 360-10 was used, both the EC 3 and the NIST models accurately predict the buckling temperature of the tested column specimen with difference less than 5% on average.

INTRODUCTION

Calculation methods are often adopted to determine the fire protection for steel structures as opposed to conducing costly experiments. Accurate high temperature constitutive models are required to reasonably predict the structural performance

chao.zhang@nist.gov; lisa.choe@nist.gov; john.gross@nist.gov
Engineering Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899, U.S.A

Zhang, Chao; Choe, Lisa; Gross, John.
"High-temperature material constitutive models for structural-fire analysis."
Paper presented at the 9th International Conference on Structures in Fire SiF'16, Princeton, NJ, Jun 7-Jun 10, 2016.

under fire conditions. As part of the investigation on the collapse of the World Trade Center, the National Institute of Standards and Technology (NIST) characterized the steels recovered from the collapse site to analyze the failure induced by the air-craft impact and fire. In the investigation [5], the high-temperature tensile testing was conducted following ASTM E21 [6]. With the test data in the investigation and the data found in the technical literature, a new constitutive model, referred to as the NIST steel stress-strain model or NIST model in this paper, was developed to predict the high-temperature behavior of structural steels [1,7]. This paper compares the NIST model with the two widely used constitutive models, the Eurocode 3 model [2] and the TTLie model [3], for predicting the behavior of steel components under fire conditions. The constitutive models are used to predict the buckling temperature of steel columns and the response of restrained steel beams under uniform fire condition. In this paper, buckling temperature is defined as the steel temperature at the onset of buckling.

STEEL STRESS-STRAIN MODELS

Mathematical formulation

Detailed description of the NIST model can be found in Ref.[8]. The stress-strain expressions for the NIST model is given in Eq.1,

$$\sigma = \begin{cases} \varepsilon E_T \quad (\varepsilon \leq \dfrac{f_{yT}}{E_T}) \\ f_{yT} + (k_3 - k_4 f_{y20}) \exp[(\dfrac{T}{k_2})^{k_1}](\varepsilon - \dfrac{f_{yT}}{E_T})^n \quad (\varepsilon > \dfrac{f_{yT}}{E_T}) \end{cases} \tag{1}$$

where k_1=7.82, k_2=540°C, k_3=1006 MPa, k_4=0.759, and n=0.503. The elastic modulus and yield strength at elevated temperature are calculated by

$$\frac{E_T}{E_{20}} = \exp[-\frac{1}{2}(\frac{T-20}{639})^{3.768} - \frac{1}{2}(\frac{T-20}{1650})] \tag{2}$$

and

$$\frac{f_{yT}}{f_{y20}} = \exp[-\frac{1}{2}(\frac{T-20}{590})^{5.7} - \frac{1}{2}(\frac{T-20}{919})] \tag{3}$$

where E_{20}, E_{T} are elastic modulus of steel at ambient and elevated temperatures, respectively; and $f_{\mathrm{y}20}$, f_{yT} are yield strength of steel at ambient and elevated temperatures, respectively.

The expressions for the Eurocode 3 model and the TTLie model can be found in Refs.[2] and [3], respectively.

Compare with material test data

Figure 1 compares the calculated reduction factors for elastic modulus and yield strength with the test data collected by Luecke et al. [1]. The NIST model shows good agreement with the test data.

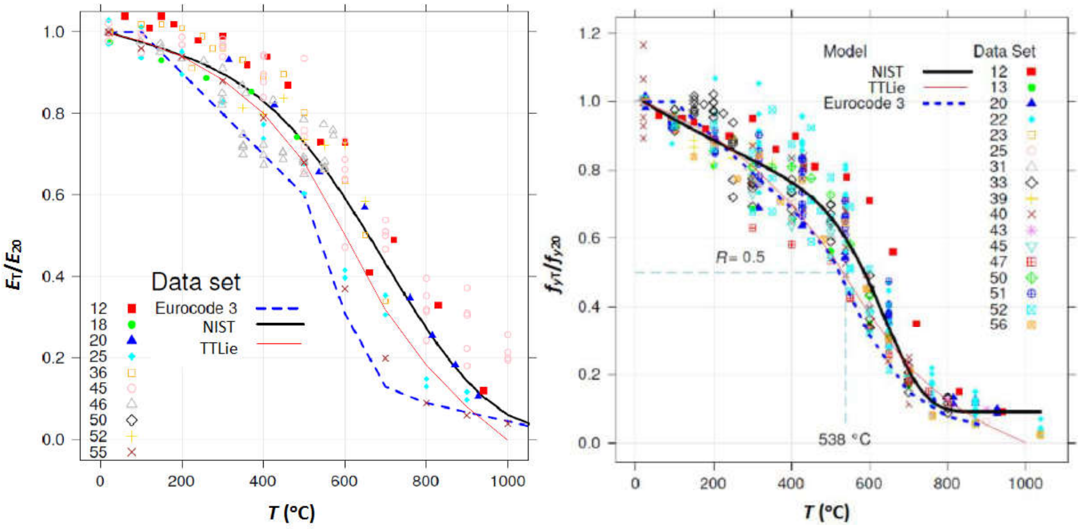


Figure 1. Calculated reduction factors for elastic modulus and yield strength against the test data collected by Luecke et al. [1]. The test labels are the same as in Ref. [1].[1]

CALCULATION APPROACHES

Eurocode 3 design approach

Simple analytical approaches given in the design codes are mostly used in daily design work. The simple approach developed by Franssen et al. [9] is recommended in the Eurocode 3 [2] for calculating the buckling resistance of axially loaded steel columns in fire, which is given by

$$N_{b,T} = \chi_T A f_{yT} \tag{4}$$

with

$$\chi_T = \frac{1}{\varphi_T + \sqrt{\varphi_T^2 - \overline{\lambda}_T^2}} \tag{5}$$

$$\varphi_T = \frac{1}{2}[1 + \alpha \overline{\lambda}_T + \overline{\lambda}_T^2] \tag{6}$$

where $\alpha = 0.65\sqrt{235 / f_{y20}}$, $\overline{\lambda}_T = \sqrt{A f_{yT} / P_{ET}}$. A is the steel cross section area and P_{ET} is Euler bucking load at elevated temperature. By solving $P_T = N_{b,T}$, we obtain the column buckling temperature. Here P_T is the column service load under fire condition.

ANSI/AISC design approach

The 2005 and 2010 editions of the ANSI/AISC-360 Appendix 4 [4] specify to use the Eurocode 3 temperature-dependent mechanical properties for design of steel

[1] The Eurocode 3 yield strength plotted here is determined at the 0.2 % offset for comparison purposes, while the high-temperature yield strength in the Eurocode 3 is defined at 2% strain.

members at elevated temperatures. According to the 2005 edition, the critical buckling stress, $F_{cr}(T)$, for steel column for fire conditions can be computed using the standard design equations (i.e., in Chapter E of the ANSI/AISC-360), as expressed in Eqs [7] through [9], with the temperature-dependent values of elastic modulus, E (T), and yield strength, F_y (T). On the other hand, the 2010 edition prescribes Eq [10] to compute flexural buckling strength of columns at elevated temperatures. The Eq [10] is valid only when Eurocode 3 mechanical properties are considered for design. Both versions of the equations use the effective column slenderness ratio, *KL/r*, which is independent of temperatures, to compute the temperature-dependent elastic buckling stress $F_e(T)$ (given in Eq [9]).

$$F_{cr}(T) = \left[0.658^{\frac{F_y(T)}{F_e(T)}} \right] \cdot F_y(T) \quad \text{for } F_e(T) \geq 0.44 F_y(T) \tag{7}$$

$$F_{cr}(T) = 0.877 \cdot F_e(T) \quad \text{for } F_e(T) < 0.44 F_y(T) \tag{8}$$

$$F_e(T) = \frac{\pi^2 E(T)}{\left(\frac{KL}{r}\right)^2} \tag{9}$$

$$F_{cr}(T) = F_y(T) \cdot 0.42^{\left(F_y(T)/F_e(T)\right)^{0.5}} \tag{10}$$

FE approach

COLUMN MODEL

The three-dimensional shell element, SHELL181, implemented in ANSYS 14.0.0 [10] was used since this element is suitable for analyzing thin to moderately thick shell structures. The column cross sections were discretized into twenty elements based on mesh optimization study. The shape of initial column crookedness was defined as the first mode obtained from elastic buckling analysis. The initial deflection amplitude at mid-height, if not specified, was taken as $L/1000$. Neither the effect of residual stress due to cooling of the hot-rolled shape nor the thermal gradient from fire was modeled explicitly. The buckling temperature of columns was computed from the point at which the force equilibrium could not be achieved.

RESTRAINED BEAM MODEL

Figure 2 shows a FE structural model for a restrained steel I-shaped beam. The steel beam was modeled using SHELL181, and the restraints at the beam ends were modeled using spring-damper element COMBIN14. As shown at the right corner in Figure 2, an axial spring and a rotational spring located at mid-height of the beam end section were used to provide axial and rotational restraints, respectively. This approach can be used to model various end conditions.

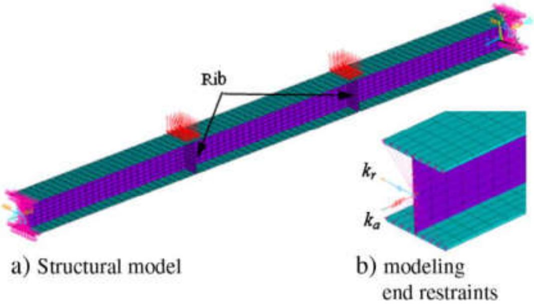


Figure 2. FE model of a restrained steel I beam.

TEST DATA

Steel columns

The five column data sets, which were selected from Zhang et al. [11], were used for FE simulations and design calculations, Table II shows a total of twenty individual column specimens along with the reported failure temperatures ($T_{b,meas}$) and other test parameters, such as the ambient temperature yield strength (f_{y20}), column length (L),slenderness ratio ($\lambda = L/r$, where r is the radius of gyration), the applied axial load(P_T), the boundary conditions (ends, where P-P is pinned-pinned; F-F is fixed-fixed; and P-R is pinned-rotationally restrained), and the initial eccentricity (e).

TABLE II. STEEL COLUMN TEST DATA.

Data	**Test**	**Shape**	f_{y20}	L	λ	P_T	**e**	**Ends**	$T_{b,mea}$
			(MPa	(mm)		(kN)	(m		(°C)
Ali [12]	Ali1	UC152×152×23	320	1800	47	186	0	P-P	701
	Ali2	UC152×152×23	320	1800	47	373	0	P-P	626
	Ali3	UC152×152×23	320	1800	47	559	0	P-P	557
	Ali4	UB178×102×19	320	1800	75	202	0	P-P	629
	Ali5	UB178×102×19	320	1801	75	303	0	P-P	539
	Ali6	UB178×102×19	320	1802	75	101	0	P-P	644
	Ali7	UB127×76×13	320	1803	97	50	0	P-P	717
	Ali8	UB127×76×13	320	1804	97	101	0	P-P	658
	Ali9	UB127×76×13	320	1805	97	151	0	P-P	567
Choe[13]	1	W8×35	413	3500	67.	1134	0	P-P	500
	2	W8×35	413	3500	67.	800	0	P-P	600
	3	W14×53	406	3450	70.	1435	0	P-P	500
	4	W14×53	406	3450	70.	1070	0	P-P	600
Lie [2]	Lie1	W10×60	300	3810	34	1760	0	F-F	565
	Lie2	W10×49	300	3810	34	1424	0	F-F	586
	Lie3	W10×49	300	3810	34	1424	0	F-F	584
Tan [14]	RS45	UC152×152×37	326	1500	38	708.5	1.74	P-P	647
	RS55	UB203×133×25	357	1500	47	444.3	3.19	P-P	571
	RS81	UB152×89×16	312	1500	70	260.6	2.38	P-P	499
	RS97	UB127×76×13	320	1500	83	134	4.08	P-P	606

*Note: Ali, Lie, and Tan - transient tests; Choe - steady state tests.

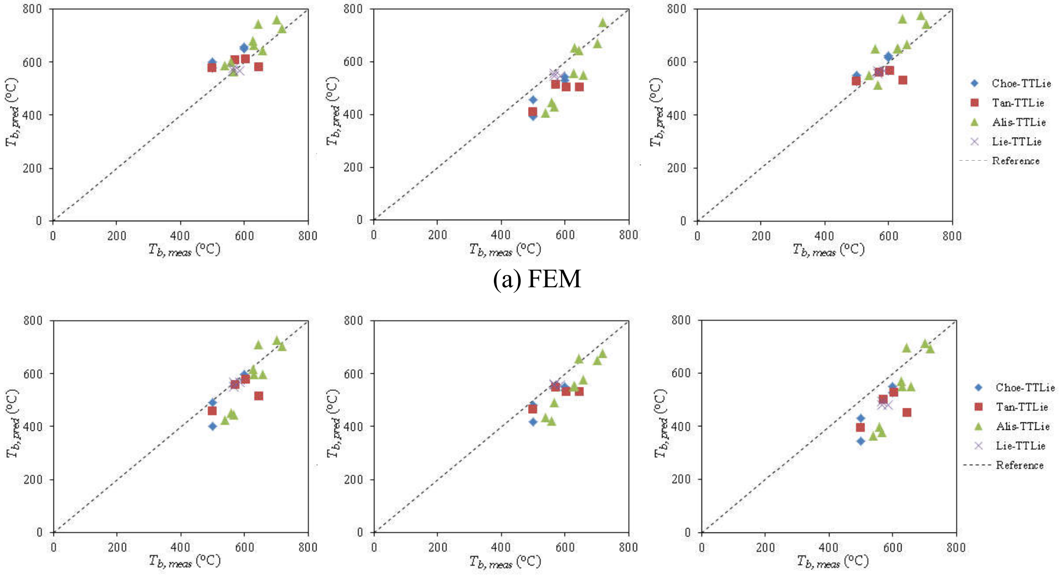
Restrained steel beams

Two tests were considered to evaluate the response of restrained beams in fire. Test on specimen 1 in Li and Guo [15] and test on "FUR15" in Liu et al.[16] were considered. In [15], the tested beam had a cross section H250×250×8×12 and a clear span length of 4500 mm. Two concentrated loads were applied symmetrically on the restrained beam by two jacks. The space between these two point loads was 1500 mm. The load ratio of the restrained beam was 0.7. The axial stiffness provided by the restrained frame was k_a=39.54 kN/mm and the rotational stiffness was k_r=1.09×10^8 Nm/rad. In [16], the tested beam had a cross section 178×102×19UB and a clear span length of 2000 mm. Two symmetrical concentrated loads were applied. The space between these two point loads was 800 mm. The load ratio of the restrained beam was 0.5. End-plate beam-to-column connections were used. The axial stiffness provided was k_a=8 kN/mm and the rotational stiffness was k_r=1.4×10^5 Nm/rad.

RESULTS

Buckling temperatures

Figure 3 shows comparisons among the predicted and measured values for column buckling temperature by using different material models. Table III shows the statistics of the ratios of the difference among the analytical results and measured data for different material models. The mean and standard deviation (Std) are presented in the table. For FE approach, all three models give acceptable predictions, and NIST and TT Lie models give better prediction than the EC3 model. For Eurocode 3 approach, all three models give under-predictions, and NIST and EC3 models give better prediction than the TT Lie model.



(a) FEM

(b) Eurocode 3 method

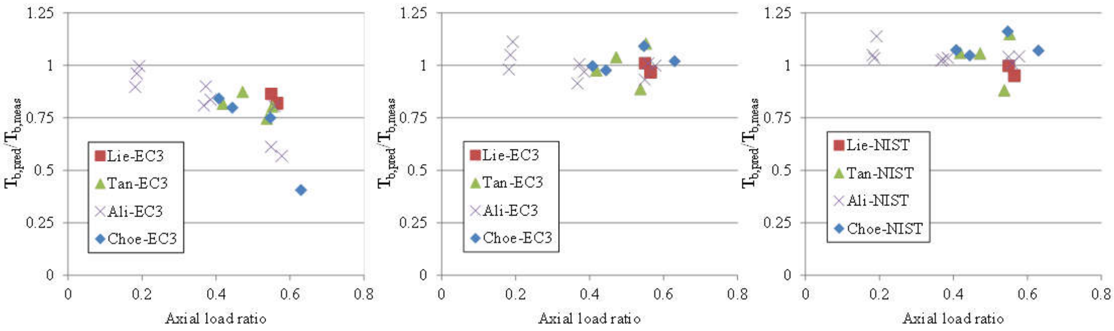
Figure 3. Column buckling temperatures predicted using FEM (a) and Eurocode 3 method (b).

TABLE III. STATISTICS OF THE RATIOS OF THE DIFFERENCE AMONG THE ANALYTICAL RESULTS AND MEASURED DATA*.

Statistics	***NIST***	***EC3***	***TT Lie***
FEM: mean	0.060	0.110	0.024
FEM: standard Std	0.075	0.091	0.084
Eurocode 3: mean	-0.066	-0.096	-0.156
Eurocode 3: standard Std	0.091	0.068	0.113

*Note: the ratio is defined as $(T_{b,pred} - T_{b,meas})/T_{b,meas}$.

Figure 4 shows that the current ANSI/AISC 360-10 Appendix 4 equation conservatively estimate the buckling temperature of the tested column specimens with difference of 20% on average (Figure 4a). When the standard column equation in the Chapter E of ANSI/AISC 360 was used, both the EC 3 and the NIST models accurately predict the buckling temperature of the tested column specimen with the difference less than 5% on average (Figure 4b).



(a) Appendix 4

(b) Chapter E

Figure 4. Column buckling temperature predicted using ANSI/AISC-360 (a) Appendix 4 (b) Chapter E.

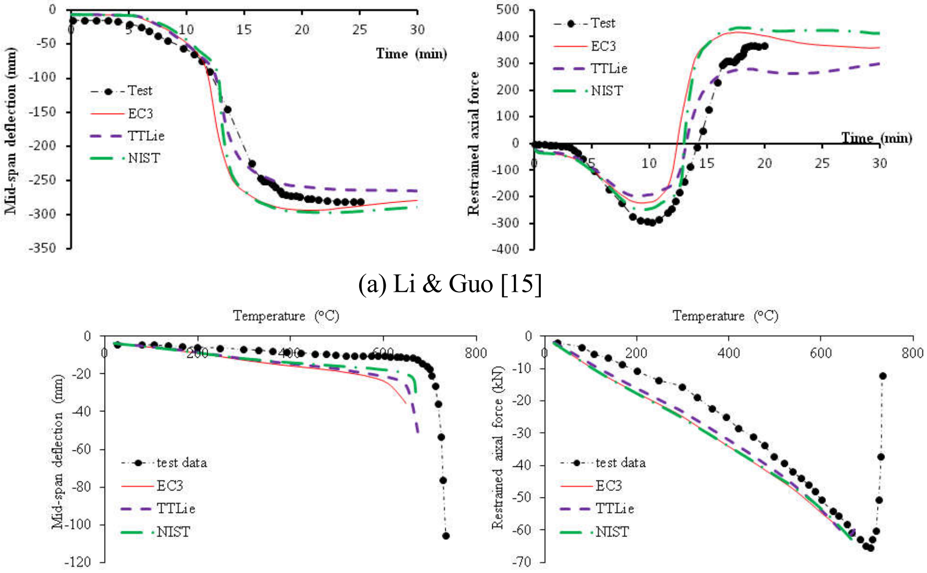
Response of restrained beam

Figure 5 show the FE predicted results for the restrained steel beam. All three material models give good prediction of the response of the restrained beams.

CONCLUSIONS

A comparative study of three high temperature steel constitutive models for structural fire analyses was presented. All investigated material models give acceptable prediction of the buckling temperature of steel columns. For the FE approach, using NIST and TTLie models give better prediction than the EC3 model; and for the Eurocode analytical approach, NIST and EC3 models give better prediction than the TTLie model. All three models give good prediction of the response of restrained steel beams subjected to fire.

DISCLAIMER Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.



(a) Li & Guo [15]

(b) Liu et al. [16]

Figure 5. FE results for restrained force and mid-span deflection for restrained steel beam.

REFERENCES

1. Luecke W E, Banovic SW, McColskey JD (2011). “High-temperature tensile constitutive data and models for structural steels in fire,” NIST Technical Note 1714.
2. ECS (2005). Eurocode 3. "Design of steel structures. General rules. Structural fire design," Standard EN 1993-1-2, European Committee for Standardization.
3. Lie TT, Macaulay JD (1989). “Evaluation of the fire resistance of protected steel columns,” Internal Report No. 583, National Research Council Canada.
4. AISC (2005, 2010). “Specification for structural steel buildings,” Specification ANSI/AISC 360-10, American Institute of Steel Construction (AISC).
5. NIST (2005). "Federal building and fire safety investigation of the World Trade Center disaster: Mechanical properties of structural steel," Technical Report NCSTAR 1-3D.
6. ASTM International (2009). “Standard test methods for elevated temperature tension tests of metallic materials.” Standard E21-09, ASTM International, W. Conshohocken, Pa.
7. Choe L, Zhang C, Luecke WE, Gross JL, Varma AH (2016). “Influence of material models on predicting the fire behavior of steel columns,” *Fire Technol.,* DOI: 10.1007/s10694-016-0568-4.
8. NIST (2016) “Temperature-dependent material modeling for structural steels: formulation and application.” NIST Technical Note 1907.Doi: 10.6028/NIST.TN.1907
9. Franssen JM, Schleich JB, Cajot LG, Azpiazu W (1996). "A simple model for the fire resistance of axially-loaded members - comparison with experimental results," *J. Constr. Steel. Res*., 37:175-204.
10. ANSYS (2012) ANSYS User Manual Version 14.0.
11. Zhang C, Li GQ, Wang YC (2012). "Predictability of buckling temperature of axially loaded steel columns in fire," *J. Constr. Steel. Res*., 75:32-7.
12. Ali FA, Shepherd P, Randall M, Simms IW, O’Connor DJ, Burgess I (1998). "Effect of axial restraint on the fire resistance of steel columns," *J. Constr. Steel. Res*., 46:305-6.
13. Choe L, Varma AH, Agarwal A, Syrovek A (2011). "Fundamental behavior of steel beam-columns and columns under fire loading: experimental evaluation," *J. Struct. Eng.-ASCE*, 137:954-66.
14. Tan KH, Toh WS, Huang ZF, Phng GH (2007). "Structural responses of restrained steel columns at elevated temperatures. Part 1: Experiments," *Eng. Struct.*, 29:1641-52.
15. Li GQ, Guo SX (2008). "Experiment on restrained steel beams subjected to heating and cooling," *J. Constr. Steel. Res*., 64:268-74.
16. Liu TCH, Fahad MK, Davies JM (2002). "Experimental investigation of behavior of axially restrained steel beams in fire," *J. Constr. Steel. Res*., 58:1211-30.