Industrial Control System Security and NIST SP 800-53 Overview

July 2, 2008

Keith Stouffer
Stu Katzke
National Institute of Standards and Technology

Keith Stouffer

- Mechanical Engineer in the Intelligent Systems Division within the NIST Manufacturing Engineering Laboratory – 17 years
- Program Leader of the Industrial Control System Security and Industrial Network Standards Program
- Member of ISA99 (WG4 and WG5)
- US TAG member for IEC/TC 65 and IEC/SC 65C
- Bachelor's Degree in Mechanical Engineering from the University of Maryland
- Master's Degree in Computer Science from Johns Hopkins University

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Stu Katzke

- Retired from NIST as a Senior Research Scientist after a 33 year career in the U.S. Government—over 30 at NIST (7 years)
- Post-retirement: Working for NIST under direct contract & as Guest Researcher.
- Co-project lead (with Keith Stouffer) of the ITL/MEL Industrial Control System Security Project, NIST (2-3 years)
- Chief Scientist of the Information Assurance Solutions Group, NSA (2 ½ years)
- Chief of the Computer Security Division, NIST (12 years)
- Manager, Computer Security Management & Assistance Group, NIST (7 years)
- Assistant Professor, College of William & Mary (3 years)
- Ph.D. Information Science, Case Western Reserve University (1973)

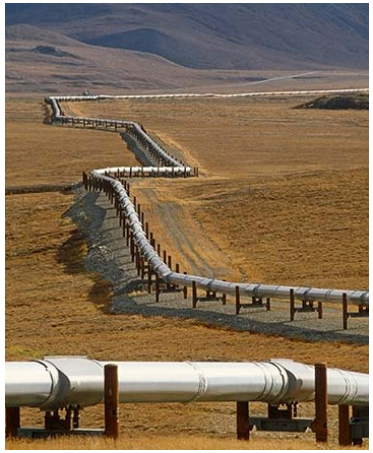
NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Industrial Control Systems (ICS) Overview

- **Industrial Control System (ICS)** is a general term that encompasses several types of control systems including:
  - Supervisory Control and Data Acquisition (SCADA) systems
  - Distributed Control Systems (DCS)
  - Other control system configurations such as skid-mounted Programmable Logic Controllers (PLC)
- ICS are specialized Information Systems that physically interact with the environment
- Many ICS are components of the Critical Infrastructure

SCADA Examples

SCADA systems are used in the electricity sector, oil and gas pipelines, water utilities, transportation networks and other applications requiring remote monitoring and control.



Typical Control Room Layout

Control room provides network status, enables remote control, optimizes system performance, facilitates emergency operations, dispatching repair crews and coordination with other utilities.

Typical Operator Interface

Displays real-time network status on Geographic and schematic maps

Provides control of circuit breakers, switches, etc.

Displays dynamic coloring to show real-time changes

Provides alarm status

Provides optimization functions and decision making support

Typical RTU Hardware

Remote Terminal Unit (RTU)

Gathers data from sensors (pressure, flow, voltage, etc.) and controls local actuators (pumps, valves, breakers, etc.)

DCS Examples

Electric Power Generation

Manufacturing

Refineries

Industrial Control System Security Challenges

- Real time constraints - IT security technology can impact timing, inhibit performance (response times are on the order of ms to s)
- Balancing of performance, reliability, flexibility, safety, security requirements
- Difficulty of specifying requirements and testing capabilities of complex systems in operational environments
- Security expertise and domain expertise required, but are often separated

Information Technology vs. Industrial Control Systems

Different Performance Requirements

Information Technology	Industrial Control
Non-Realtime	Realtime
Response must be reliable	Response is time critical
High throughput demanded	Modest throughput acceptable
High delay and jitter accepted	High delay and/or jitter is a serious concern

Information Technology vs. Industrial Control Systems

Different Reliability Requirements

Information Technology	Industrial Control
Scheduled operation	Continuous operation
Occasional failures tolerated	Outages intolerable
Beta testing in the field acceptable	Thorough testing expected

Information Technology vs. Industrial Control Systems

Different Risk Management Requirements: Delivery vs. Safety

Information Technology	Industrial Control
Data integrity paramount	Human safety paramount
Risk impact is loss of data, loss of business operations	Risk Impact is loss of life, equipment or product, environmental damage
Recover by reboot	Fault tolerance essential

These differences create huge differences in acceptable security practice

Gasoline Pipeline Failure

- **Event**: Gasoline pipeline failure exacerbated by control systems not able to perform control and monitoring functions
- **Industry**: Gasoline Pipeline
- **Location**: North America
- **Information Source**: NTSB Final Report
- **Impact**: 3 fatalities, total property damage >$45M
- **Lessons learned**:
  - Do not perform database update development while system in operation.
  - Apply appropriate security to remote access

Water Storage Dam Failure

- **Event**: Remotely controlled Pumped Storage Dam Failure (Dec 14, 2005) due to instrument failure
- **Industry**: Hydro Storage Plant
- **Location**: North America
- **Information Source**: Utility & FERC
- **Impact**:
  - Loss of >450 MW hydro station
  - Environmental and economic loss still being evaluated
- **Lessons learned**:
  - Hardwired safety systems could prevent catastrophic events
  - Secure/Insure instrumentation

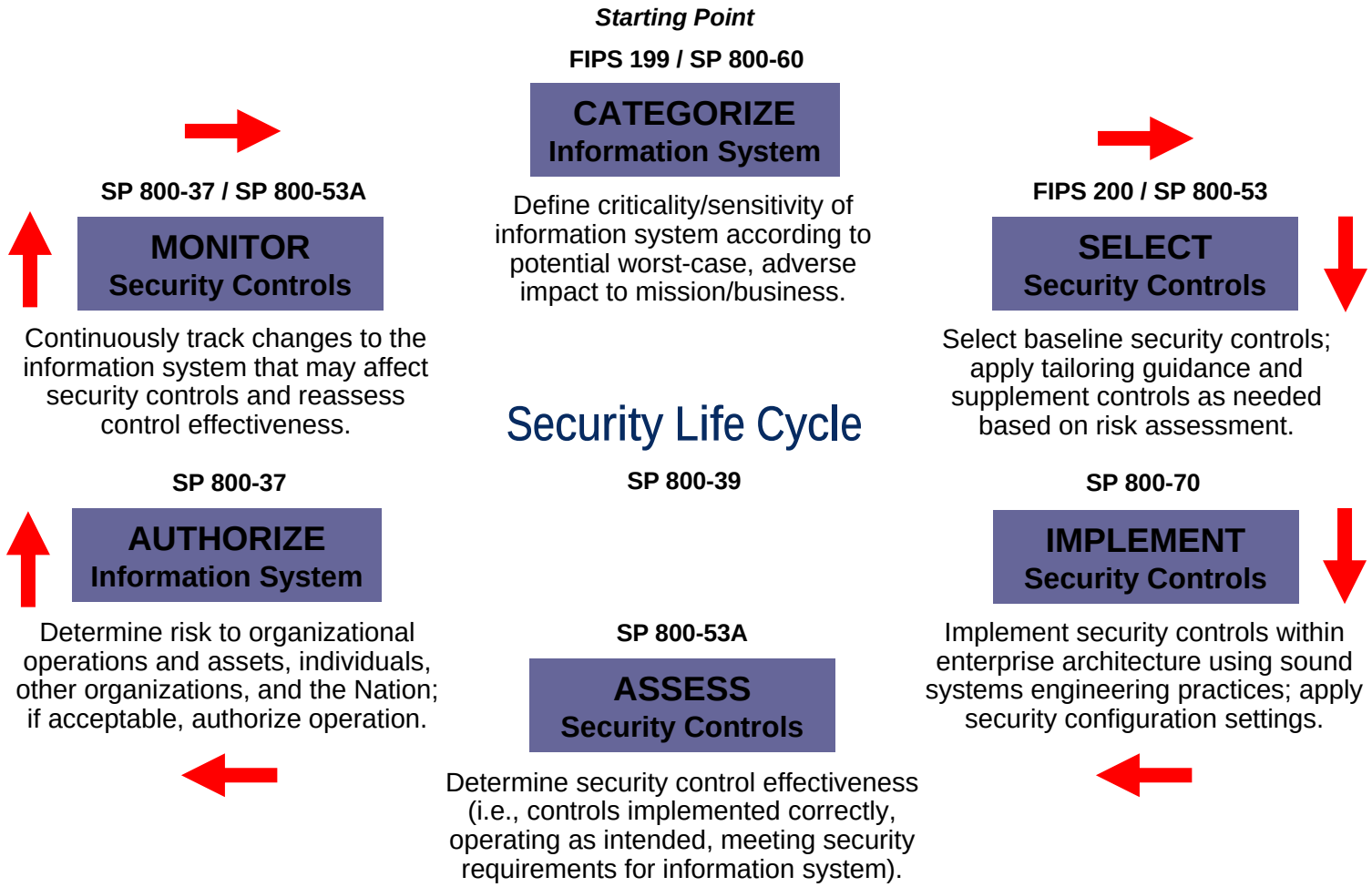
U.S. Federal ICS Security Standards and Guidelines

NIST Industrial Control System (ICS) Security Project

- Joint MEL/ITL project, in collaboration with federal and industry stakeholders, to develop standards, guidelines and test methods to help secure these critical control systems in harmony with their demanding safety and reliability requirements.

http://csrc.nist.gov/sec-cert/ics

NIST Risk Management Framework

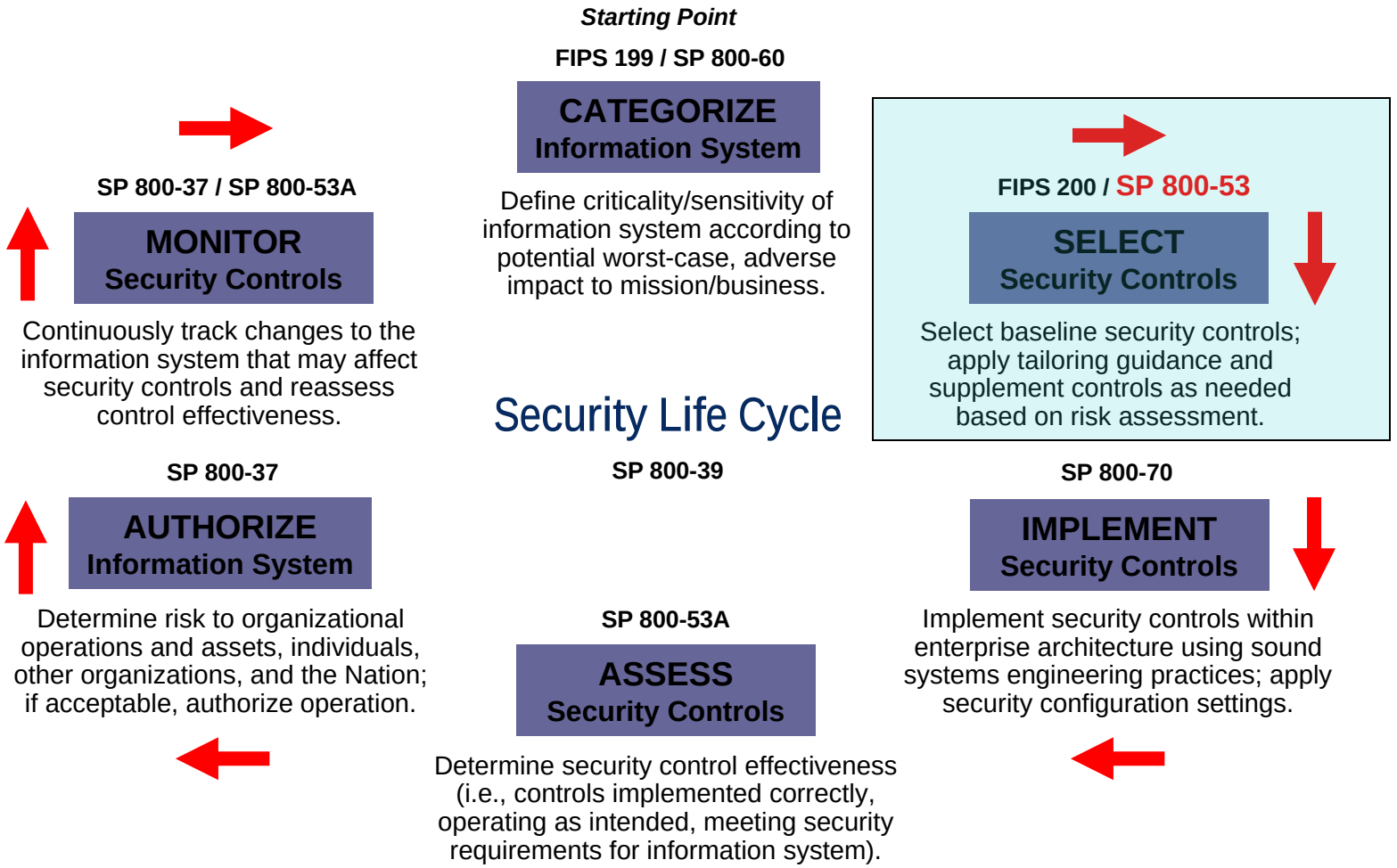


U.S. Federal ICS Security Standards and Guidelines Strategy

- Add control systems domain expertise to:
  - Already available IT security Risk Management Framework
  - Provide workable, practical solutions for control systems – without causing more harm than the incidents we are working to prevent

- This expertise takes the form of specific cautions, recommendations & requirements for application to control systems - throughout both technologies and programs
  - ICS Augmentation of NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*
  - NIST SP 800-82 *Guide to Industrial Control System (ICS) Security*

NIST Risk Management Framework



NIST SP 800-53

- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*, which was developed for traditional IT systems, contains mandatory information security requirements for all non-national security information and information systems that are owned, operated, or controlled by federal agencies.

- NIST SP 800-53 provides the security controls that need to be applied to secure the system. It does not specify how the controls need to be implemented.

NIST SP 800-53 Organization

17 Control Families
171 Controls (Requirements)

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental
- Planning
- Personnel Security
- Risk Assessment
- Systems and Services Acquisition
- System and Communications Protection
- System and Information

NIST SP 800-53 Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

NIST SP 800-53 Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

NIST SP 800-53 Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

NIST SP 800-53 Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

NIST SP 800-53 Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

NIST SP 800-53 Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

Augmenting NIST SP 800-53 to address ICS

- NIST SP 800-53 contains mandatory information security requirements for all non-national security information and information systems, including ICS, that are owned, operated, or controlled by federal agencies.
- When organizations attempted to utilize SP 800-53 to protect ICS, it led to difficulties in implementing SP 800-53 counter-measures because of ICS-unique needs.
- Held 2 Workshops (April 2006 and March 2007) with stakeholders to discuss issues and develop ICS material for SP 800-53. 2 drafts were released for public vetting before SP 800-53, Rev 2 was finalized December 2007.

Changes made to NIST SP 800-53

- Original NIST SP 800-53 controls were not changed
- Additional guidance was added to address ICS
  - ICS Supplemental Guidance
  - ICS Enhancement Supplemental Guidance
- Additional guidance provides information on how the control applies in ICS environments, or provides information as to why the control may not be applicable in ICS environments.
- Additional guidance was added to 65 of 171 controls

Example ICS Supplemental Guidance

CA-2 SECURITY ASSESSMENTS

ICS Supplemental Guidance:

The assessor fully understands the corporate cyber and ICS security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before the assessments can be conducted. If a ICS must be taken off-line for assessments, assessments are scheduled to occur during planned ICS outages whenever possible.

Example ICS Supplemental Guidance

SC-13 USE OF CRYPTOGRAPHY

ICS Supplemental Guidance:

ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

Key Take Away

- NIST SP 800-53, Revision 2 is a security standard that addresses both general IT systems as well as ICS. This allows the federal agencies, as well as the private sector if desired, to use one document to determine the proper security controls for their IT systems as well as to effectively secure their industrial control systems while addressing their unique requirements.

- NIST SP 800-53, Revision 2 available at:
  - http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

Federal ICS using NIST SP 800-53, Revision 2

- Bonneville Power Administration (BPA)
- Southwestern Power Administration (SWPA)
- Tennessee Valley Authority (TVA)
- Western Area Power Administration (WAPA)
- Federal Aviation Administration (FAA)
- Department of the Interior, Bureau of Reclamation

NIST SP 800-53 Security Baselines

- LOW Baseline - Selection of a subset of security controls from the master catalog consisting of ***basic*** level controls
- MOD Baseline - Builds on LOW baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***
- HIGH Baseline - Builds on MOD baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***
- Categorization based on the potential level of impact if the **Availability, Integrity or Confidentiality** of the system or information on the system is compromised.
- ***How do we categorize ICS?***

Low Impact System

Possible ICS Impact Level Definitions

- **Low Impact**
  - **Product Controlled:** Non hazardous materials or products, Non-ingested consumer products
  - **Industry Examples:** Plastic Injection Molding, Warehouse Applications
  - **Security Concerns:** Protecting people, Capital investment, Ensuring uptime

Moderate Impact Systems

Possible ICS Impact Level Definitions

- **Moderate Impact**
  - **Product Controlled:** Some hazardous products and/or steps during production, High amount of proprietary information
  - **Industry Examples:** Automotive Metal Industries, Pulp & Paper, Semi-conductors
  - **Security Concerns:** Protecting people, Trade secrets, Capital investment, Ensuring uptime

High Impact System

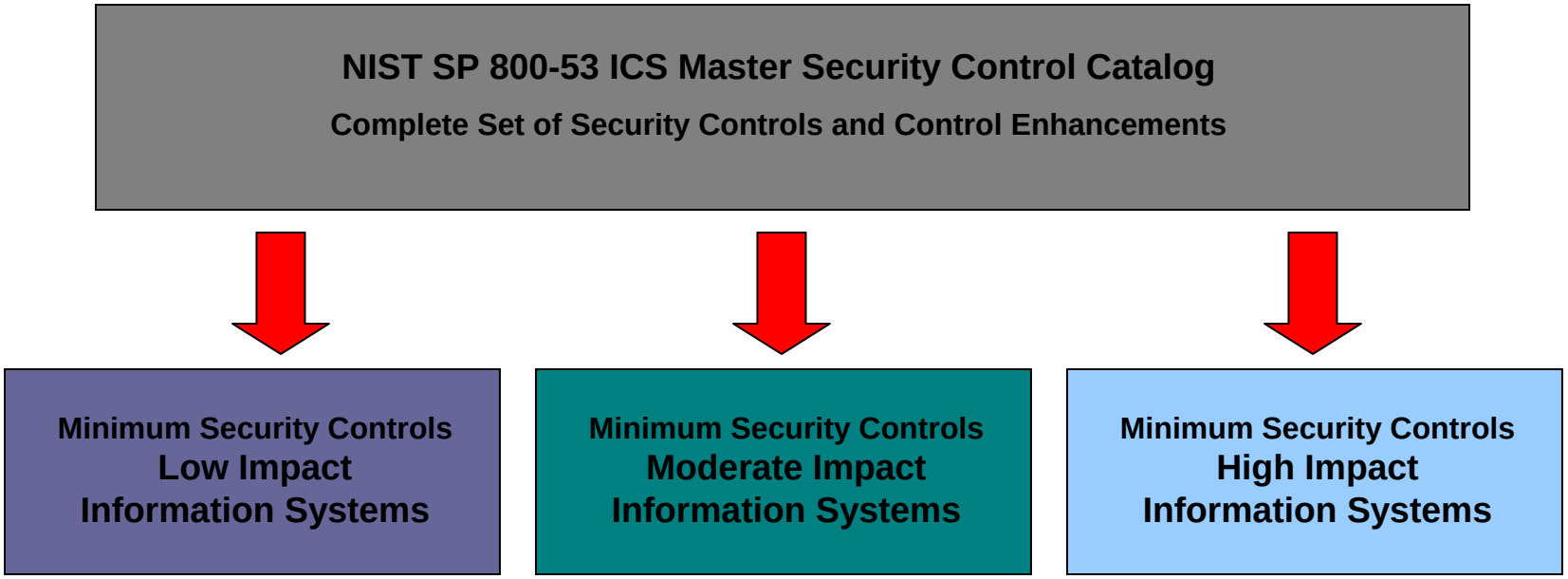
High Impact System !!!

Possible ICS Impact Level Definitions

- **High Impact**
  - **Product Controlled:** Critical Infrastructure, Hazardous Materials, Ingested Products
  - **Industry Examples:** Utilities, PetroChemical, Food & Beverage, Pharmaceutical
  - **Security Concerns:** Protecting human life, Ensuring basic social services, Protecting environment

More High Impact Systems ☺

Security Control Baselines



Baseline #1

Selection of a subset of security controls from the master catalog—consisting of ***basic*** level controls

Baseline #2

Builds on low baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Baseline #3

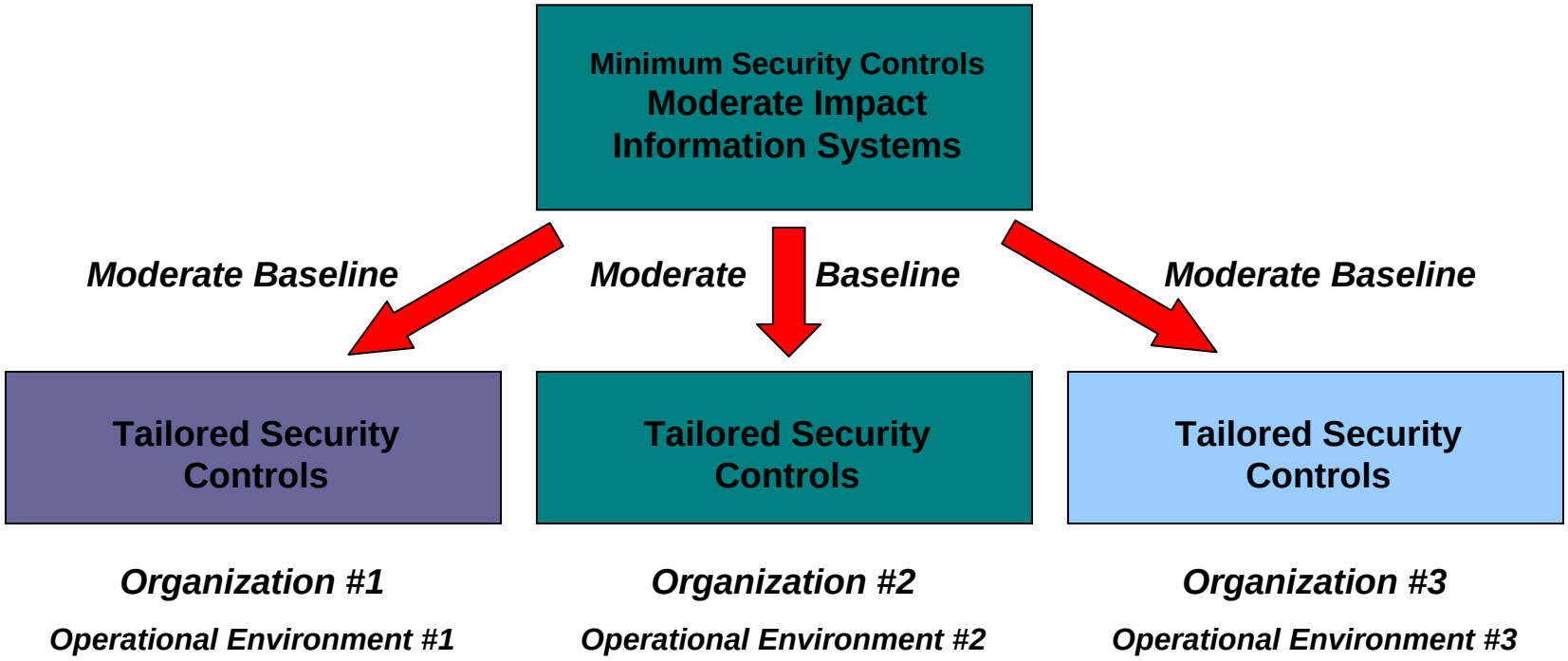
Builds on moderate baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Minimum Security Controls

- Minimum security controls, or baseline controls, defined for low-impact, moderate-impact, and high-impact information systems—
  - Provide a ***starting point*** for organizations in their security control selection process
  - Are used in conjunction with ***tailoring guidance*** that allows the baseline controls to be adjusted for specific operational environments
  - Support the organization's ***risk management process***

Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls



Cost effective, risk-based approach to achieving information security…

NIST SP 800-82

- Guide to Industrial Control Systems Security
  - Provide guidance for establishing secure ICS, including implementation guidance for SP 800-53 controls
- Content
  - Overview of ICS
  - ICS Characteristics, Threats and Vulnerabilities
  - ICS Security Program Development and Deployment
  - Network Architecture
  - ICS Security Controls
  - Appendixes
    - Current Activities in Industrial Control Systems Security
    - Emerging Security Capabilities
    - ICS in the FISMA Paradigm

NIST SP 800-82

- Initial public draft released September 2006 - public comment period through December 2006
- Second public draft released September 2007 - public comment period through November 2007
- Final public draft scheduled for June 2008
- Final document scheduled for August 2008
- Downloaded over 400,000 times since initial release
- Current document available at:
  - http://csrc.nist.gov/publications/drafts.html

Key Take Away to Securing ICS

- The most successful method for securing an ICS is to gather industry recommended practices and engage in a ***proactive, collaborative effort*** between management, the controls engineer and operator, the IT department, the physical security department, and a trusted automation advisor. This team should draw upon the wealth of information available from ongoing federal government, industry group, vendor and standards organizational activities.

Major ICS Security Objectives

- **Restricting logical access to the ICS network and network activity**
  - This includes using a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and ICS networks, and having separate authentication mechanisms and credentials for users of the corporate and ICS networks. The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restricting physical access to the ICS network and devices**
  - Unauthorized physical access to components could cause serious disruption of the ICS's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.

Major ICS Security Objectives

- **Protecting individual ICS components from exploitation**
  - This includes deploying security patches in as expeditious a manner as possible, after testing them under field conditions; disabling all unused ports and services; restricting ICS user privileges to only those that are required for each person's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware.
- **Maintaining functionality during adverse conditions**
  - This involves designing the ICS so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event.

Private Sector ICS Security Standards

- Where the rubber hits the road!
- 90+% of ICS are owned by the private sector
- Standards for the ICS industry, if widely implemented, will raise the level of control systems security
- Greatest chance for industry acceptance and adoption is to have security requirements published in cross industry standards
  - **ISA99 *Industrial Automation and Control System Security* standard**
  - **IEC 62443 *Security for Industrial Process Measurement and Control – Network and System Security* standard**

ISA99

- Co-Chairs: Bryan Singer – Wurldtech, Eric Cosman - Dow
- Developing an ANSI Standard for Industrial Automation and Control System Security
  - Part 1 – Models and Terminology
  - Part 2 – Establishing an Industrial Automation and Control Systems Program

    Part 3 – Operating an Industrial Automation and Control Systems Program
  - Part 4 – Technical Security Requirements for Industrial Automation and Control Systems

  - NIST SP800-53, Rev 2 have been provided to ISA99 as references to consider in the development of the standard

http://www.isa.org/MSTemplate.cfm?MicrosoftID=988&CommitteeID=6821

ISA99 - Part 4

- Designation:
  - ANSI/ISA-d99.00.04
- Topic:
  - Specific Technical Security Requirements for Industrial Automation and Control Systems
- Leaders:
  - Johan Nye - ExxonMobil, Kevin Staggs - Honeywell: Co-chairs
  - Dennis Holstein: Editor

How to participate in ISA99

- Send email to:
  - Bryan Singer, bsinger74@gmail.com
    Committee Co-Chairman
  - Eric Cosman, ECCosman@dow.com
    Committee Co-Chairman
  - Charley Robinson, crobinson@isa.org
    ISA Standards
  - Provide your contact information and area of expertise or interest.

IEC TC65/WG10 and IEC 62443

- Convenor: Tom Phinney (US)
- Approved work item proposal: 65/360/NP
- Object: Create a three-part standard

  "IEC 62443, *Security for industrial process measurement and control – Network and system security*"
- Scope: Establish requirements for securing access to industrial process measurement and control networks and devices on those networks

IEC 62443

- IEC 62443 *Security for industrial process measurement and control –Network and system security* standard
  - 62443-1, *Framework and threat-risk analysis*
  - 62443-2, *Security assurance: principles, policy and practice*
  - 62443-3, *Sets of security requirements for security elements in typical scenarios*

  - NIST SP800-53, Rev 2 have been provided to IEC TC65/WG10 as references to consider in the development of the standard

http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=dirwg.p&progdb=db1&ctnum=2931

IEC 62443 status and plans

- Decision made to take draft material for eventual IEC 62443-3 to ISA99/WG4, for joint development as a dual-labeled ISA standard and IEC technical specification
  - IEC TC65/WG10 contributors are already ISA99 members
  - Work on this document will be in ISA99/WG4
  - Work on IEC 62443-1 and -2 will continue in IEC TC65/WG10
  - Maintenance of joint ISA/IEC document will be in ISA; the others will be in IEC
  - Joint development as IEC 62443-3 pre-resolves conflict that would otherwise arise when ISA99.04 would be brought to IEC TC65/WG10 for promulgation as an international standard

Summary

- The most successful method for securing an ICS is to gather industry recommended practices and engage in a ***proactive, collaborative effort*** between management, the controls engineer and operator, the IT department, the physical security department, and a trusted automation advisor. This team should draw upon the wealth of information available from ongoing federal government, industry group, vendor and standards organizational activities.

NIST ICS Security Project Contact Information

Project Leaders

Keith Stouffer
(301) 975-3877
keith.stouffer@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

sec-ics@nist.gov

Web Pages

Federal Information Security Management Act (FISMA) Implementation Project

http://csrc.nist.gov/sec-cert

NIST ICS Security Project

http://csrc.nist.gov/sec-cert/ics

Thank You Very Much!