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

U.S.
Resilience
Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Smart Manufacturing
The Future of Manufacturing and Value Chain Competitiveness

INTERVIEWS

Denise Swink
CEO, Smart Manufacturing Leadership Coalition (SMLC)

Jim Davis
Vice Provost IT and CTO, UCLA, and Director and CTO, SMLC

Robert Graybill
President and CEO, Nimbis Services Inc.

The Next New Things in Risk Management

Smart Manufacturing technology promises to revolutionize supply chain operations by automating:

- End-to-end visibility across the supply chain
- Electronic chain of custody for products in the supply chain
- Track and trace capabilities
- Data collection and analysis on processes, energy and source materials used during manufacturing
- Predictive analysis through real-time simulation and modeling
- Secure B2B communications
- Reduced legacy system risks

Company Overview

The Smart Manufacturing Leadership Coalition (SMLC) is a non-profit organization comprised of manufacturing practitioners, suppliers, and technology companies; manufacturing consortia; universities; government agencies and laboratories. The goal is to build a cloud-based, open-architecture platform that integrates existing and future plant level data, simulations and systems across manufacturing seams and the entire value chain in order to orchestrate business real time action.

SMLC is committed to building a scaled, shared infrastructure called the SM Platform to significantly lower the barriers of cost and complexity for applying data analytics, modeling and simulation to manufacturing operations across the enterprise. SMLC activities focus on comprehensive technology that no one company can undertake. SMLC's industry-driven implementation agenda will achieve transformational supply chain capabilities, economic impact, manufacturing innovation and global competitiveness.

Smart Manufacturing: A Game Changer for Supply Chains

Some say that smart manufacturing (SM) is ushering in a fourth industrial revolution. After mechanization, industrialization and automation, it is the digitization and network connectivity of virtually all industrial processes and products that will change how things are invented, manufactured, shipped and sold. Smart manufacturing focuses on the enterprise — marrying data, technology (e.g. sensors, computers), modeling and cloud capabilities, and services with new business models.

When networked and integrated for manufacturing, data and information technologies bring intelligence and insight to every part of the manufacturing process. The key to this new opportunity: Creation of an open smart manufacturing platform which makes the application of these networked based information technologies affordable, accessible and agile.

What is Smart Manufacturing and Why Does It Matter?

Tomorrow's advanced manufacturing demands much greater precision, access, prevention, interoperability, safety, sustainability and dynamic management of manufacturing across the connected manufacturing value chain.

The Smart Manufacturing Platform (SM Platform) creates an internet infrastructure for manufacturing that:

- Orchestrates real-time data and information across the enterprise value chain to improve manufacturing and product performance;
- Offers rapid data and model-based testing, optimization and qualification to support the entire value chain;
- Integrates cloud-based applications into a secure and trusted environment in which security has been designed into the infrastructure, rather than bolted on; and
- Extends these capabilities to small and medium companies to make their and the overall value chain at once more productive and secure.

According to Denise Swink, CEO of the Smart Manufacturing Leadership Coalition:

> “What has been missing in manufacturing is the ability to affordably and accessibly knit together next generation capabilities in advanced sensors, controls, algorithms: modeling and simulation and manufacturing technologies with networked IT technologies, controls, modeling and simulation. Today, vendors provide customized one-off solutions that are complicated, expensive, non-replicable, non-scalable, and require enormous amounts of time for implementation. There are over 30,000 different legacy solutions running in the manufacturing sector today — designed to solve a variety of enterprise, operational and supply chain challenges. Making these programs work together is a huge challenge which even big companies can’t afford.”

Smart manufacturing capabilities enable end-to-end, real-time information sharing and communication internally within the plant and externally among the supply chain network, while maintaining secure, owner-management of data and digital resources. Importantly, better communication and information facilitates joint planning and reaction to events in real-time.

Digitization of the manufacturing process can be taken even further. Supply chains can collect and analyze data on plant operations that drive real-time improvements in production and optimize material, water and energy usage. For example, better sensing, scheduling, optimization across seams, production breaks and transactions, and demand-dynamic management can reduce idle machines and use manpower in better ways. For the companies that have embraced it, smart manufacturing creates opportunities to engage suppliers in the innovation process, improve productivity, enable and accelerate growth, facilitate greater worker and product safety, and improve the energy and environmental footprint.

Let us say a company wanted to make its plant more energy and economically efficient. For one chemical producer, a smart manufacturing application combines a new sensor system and high-performance modeling to see inside the process in business real-time and manage energy usage and therefore costs in ways that were not previously attainable. A variety of key performance indicators can be managed within a plant or across the enterprise with tremendous multiplier effects — or modified in business real-time to adjust to changes in manufacturing conditions, product specifications, environmental drivers, resource availability, etc. Moreover, the smart manufacturing system becomes a learning mechanism to continually improve performance, including insights into designs for modified or new plants.

For a large food producer, a smart manufacturing application is about exchanging real-time data with suppliers, farms, grain elevators, etc. before supplier product is even shipped — significantly improving dynamic production management; creating better supply and demand models; providing transparency, and track and trace capability back through the value chain, and optimizing with an end-to-end picture of the supply chain. It will extract key supply chain information from the supply chain: Which field and farmer grew the crops? Are the product attributes what I need? Was the product organically produced and does it meet process specifications? What was the lot size? Which grain elevator was it stored in? How was the product transported? Can my process accomodate the supplier product attributes? This information is no longer housed in independent — and sometimes difficult to access — data systems or even paper systems, but becomes part of the information flow that supports overall supply chain performance.

For a defense contractor, a smart manufacturing application collects and models line operation data with new and old sensors to better optimize upstream and downstream operations; and reduce material, energy waste and defects while optimizing product quality and yield in real time. What is ‘smart’ is deploying these systems faster, at lower cost and with infrastructure that allows them to progressively grow in data, scope and modeling sophistication. What is even smarter is that every stage informs the next, and captures and embeds that experience in future operations.

Smart manufacturing makes use of a common open platform, the SM Platform, through which companies can share data and information internally across their verticals as well as externally with their partners and suppliers. And, with ready access to a combined development and deployment infrastructure, that data can be turned into insight and a framework for action. As important, the smart manufacturing platform makes sophisticated automation and analytic capabilities available not only to large companies, but to small and medium-sized businesses, which often lack the resources and know-how to deploy these kinds of systems.

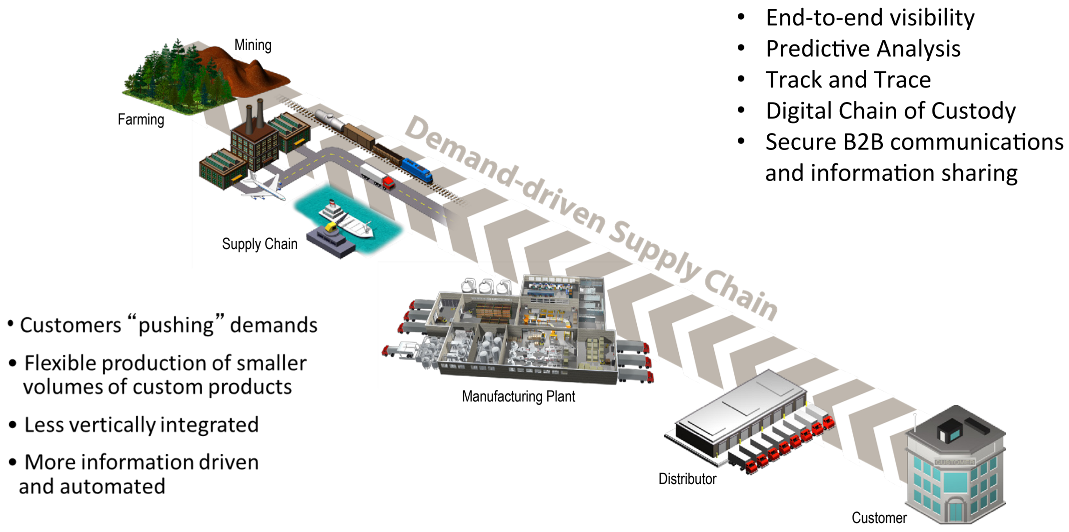
These new capabilities do require new skills and investments, and changed business models — and many manufacturers are cautious about taking on this change. Real-time and perceived cyber risks from connecting systems to each other and to the cloud add to real and perceived uncertainty and risk.

Implications for the Future of Supply Chain

Global supply chains have grown more dynamic and interdependent with higher performance demands — and as a result, there are more complex risks to manage as well as new opportunities to pursue. Through smart manufacturing, supply chains of the future can manage opportunity and risk by becoming more "instrumented, interconnected, and intelligent."[1] This impacts both supply chain effectiveness as well as supply chain security.

What will supply chains look like in a smart manufacturing world? An information-driven supply chain is more flexible and responsive to customer demand. Smart manufacturing creates capabilities and resources beyond anything available and affordable today, even for large companies. Some important capabilities include: end-to-end visibility, integrated value chain performance and predictive analysis, and reduced security and legacy system risks when increasing interoperability.

Figure 1. Demand-Dynamic Supply Chains: Efficient, Transparent, Secure
Courtesy of Rockwell Automation. © 2009 Rockwell Automation, Inc. All rights reserved.



- End-to-end visibility
- Predictive Analysis
- Track and Trace
- Digital Chain of Custody
- Secure B2B communications and information sharing

- Customers "pushing" demands
- Flexible production of smaller volumes of custom products
- Less vertically integrated
- More information driven and automated

[1] IBM Smarter Supply Chain of the Future

Supply Chains of the Future

End-to-end visibility across the supply chain (procurement, inventory, production)

This makes the entire supply chain more agile and adaptive, wrings out excess costs and builds the interoperability to ensure product value and overall manufacturing process performance. With a smart manufacturing infrastructure:

- Supply chain activities can receive and react in real time to changes in forecast demand or dynamically adjust to information from suppliers or customers.
- Real-time information throughout the supply chain provides opportunities for productivity and product improvement, creates precision information on delivery quantities and dates and reduces the need for excess inventory or premium freight expediting.

Electronic chain of custody for products in the supply chain

The end-to-end visibility and sensor technology enables 24-7 monitoring of cargo: who touched it at either end; whether the cargo has deviated from its designated route; or whether the container or package has been opened en route. Sensors provide information on cargo conditions — shock detectors, temperature, humidity, etc. These types of asset visibility measures safeguard both the physical security and quality of the shipment.

Track and trace capabilities

Supply chain visibility sets the stage for track and trace capabilities that provide a complete pedigree for manufactured products whether artifacts or materials: Who provided the materials, part or components for the product? What lot? When were they delivered? What line were they manufactured on? Which equipment they were tested on?

Integrated value chain performance

Importantly, however, smart manufacturing is much more than just data sharing and visibility. It becomes possible to analyze and model across the enterprise to address global performance objectives and take advantage of untapped opportunities for optimization.

Optimization

Enterprise interoperability sets the stage for collecting and analyzing information and data on processes, energy and source materials used during manufacture and on how the product was used and performed.

Predictive analysis

Smart manufacturing makes it possible to develop and accelerate the application of real-time analytics and modeling to form insights from operational and logistical information. Upstream and downstream interactions can be optimized and dynamically managed against energy costs. Production shipment and inventory interactions can be planned across an organization’s own enterprise as well as their trading partners. As companies analyze real-time data and understand its context in relation to operations, it becomes possible to move into predictive opportunities or address problems before they even begin.

Reduced Security and Legacy System Risk

Secure B2B communications, information sharing and operations

Value chain visibility, performance, and prediction depend on secure, owner-managed and trusted sharing of valuable information assets with supply chain partners. An environment that depends on data sharing needs to be able to prevent, detect and manage cyber attacks. When data is shared between two companies, there is always a potential risk, particularly if one side of the connection is less secure or if a third party is handling the data. Moreover, the data interfaces and connections between B2B or vendor applications can themselves become points of cyber vulnerability. The SM Platform provides an established secure environment in which to share critical data — and the security protocols for collecting, analyzing and acting on data are already in place. This avoids the need for companies to develop secure B2B connections each time.

Reduced legacy system risks

Some software, systems and equipment have been in place long enough that user companies and associated vendors are limited in their ability to maintain them. The SM Platform can provide the rationale to justify the ROI for replacing out-of-date software, systems and equipment to streamline and modernize automation processes. But, it is not necessary to begin with a major overhaul. In fact, the best approach for a business is to apply SM capabilities to a smaller, well-defined use case, understand the strengths and opportunities, create an integration team to own and execute the SM use case, and then develop a strategic approach to expand to additional use cases of pressing priority.

Benefits of Smarter Supply Chains

IBM's map of the supply chain future expresses these kinds of areas in greater detail and is a good summary of the full potential of digitizing the manufacturing enterprise supply chain. While interrelated, each category is a large challenge in its own right. Smart manufacturing effectively encompasses the portfolio with an enterprise application endgame while focusing on the infrastructure for prioritizing functionality to specific needs and progressively building toward extensive deployment and broadened functionality with tools to accelerate time to deployment, increase ROI and manage risk with rapidly changing IT.

Figure 2. The "Smartmap" to the Supply Chain of the Future: Which Capabilities are Most Critical to Your Organization?

Source: IBM Smarter Supply Chains of the Future

SCM Competency Areas	Instrumented	Interconnected	Intelligent
Strategy	▪ Visibility and performance management ▪ SC optimization and transparency ▪ Sensors and simulators of customer demand	▪ Alignment of business and SC strategies with partners ▪ Integrated sustainability strategies	▪ Variable cost structures that fluctuate with market demand
Planning	▪ Real-time demand management and inventory optimization ▪ Real-time inventory pipeline visibility ▪ Early warning detection: supply and demand synchronization	▪ Collaborative planning and execution ▪ Integration of financial and operational analysis ▪ Integrated S&OP with external metrics	▪ S&OE (where "E" is execution) ▪ Risk-adjusted inventory optimization ▪ Networked S&OP with optimized decision support
Lifecycle Management	▪ Predictive analysis and simulation design techniques ▪ Embedded systems ▪ Sensors for preventative maintenance	▪ Collaborative development and engineering with customers and partners ▪ Customer insight driving brand brilliance ▪ Knowledge sharing for continuous improvement	▪ New product development innovation and analytics ▪ Sustainable, "green" considerations throughout lifecycle ▪ Model-driven systems engineering

SCM Competency Areas	Instrumented	Interconnected	Intelligent
Sourcing and Procurement	▪ Risk and compliance sensors and modeling ▪ Proactive and real-time supply network event monitoring ▪ Global sourcing and import logistics KPIs and detection	▪ Real-time visibility of multitiered supply ▪ Contract management and strategic sourcing ▪ Outsourcing to share risks across the global network and create variable structures	▪ Predictive buy-sell analytics ▪ Sustainable procurement practices ▪ Intelligent spend analysis
Operations	▪ Optimized inventory controls and event detection ▪ Sensors and actuators in production for carbon, water, waste monitoring ▪ Visibility for operational risk management and control	▪ Networked design for manufacture, supply, use, and reuse ▪ Trade terms management linked to partnered KPIs ▪ Demand-driven production and postponement	▪ SC models to manage capital expenditure ▪ Disaster response models ▪ Simulation model to evaluate flexibility factors: service levels, costs, time, quality
Asset Management	▪ Total cost management dashboards ▪ Environmentally sustainable asset monitoring ▪ Integrated probability-based risk assessment	▪ Integrated asset and resource management ▪ Geographic information systems ▪ Dynamic and variable asset cost structures	▪ Cost-of-ownership analysis ▪ Tax and compliance modeling ▪ Proactive redeployment / reconfiguration / divesting of assets
Logistics	▪ Event-driven logistics alerts ▪ Real-time sensors for optimized network ▪ Ease of network onboarding and automated data feeds from logistics partners	▪ Real-time visibility to logistics providers ▪ Network integration with variable contingency plans and policies ▪ Agile, on-demand logistics network	▪ Carbon footprint management ▪ Data-driven reverse logistics ▪ Network and distribution strategy analysis and modeling
Enterprise Applications	▪ Monitoring and real-time detection and alerts ▪ Inventory optimization ▪ ERP to MES integration	▪ Collaboration platforms: customer, provider, supplier ▪ ERP to ERP integration ▪ Enterprise and network performance management	▪ Business intelligence and integrated analytics ▪ Predictive analysis and advanced analytics applied to events ▪ KPI trends linked to training and change management program

Security Concerns around Smart Manufacturing

Manufacturers are appropriately cautious about security of valuable data, information and IP, and security with respect to cyberattacks with network-based operations. Security is a major aspect of advanced manufacturing in general that needs to be resolved for manufacturers to operate individually and interoperate with other manufacturers securely in networked, multi-vendor, cloud-based environments. Transitioning even data and operational decision making within a manufacturing supply chain enterprise to the SM Platform, or any platform infrastructure, requires internal and external trust, confidence and understanding that the benefits far outweigh the security risks since there is always some risk. Furthermore, security is an ever changing, increasingly sophisticated function; it is a combination of technology, practice and knowledge. There is no such thing as a 100 percent secure networked based operation, and detection and mitigation are as important as prevention.

There is no question that smart manufacturing or any cloud-based operational service opens up a potential for cyber risks. This is far from a new trend, however. For the last 40 years, manufacturers have been integrating computer technologies, control systems and automation systems into their operations and connecting these systems to intranets and the Internet. Automation and control systems have generally moved to common operating systems. There are thousands of applications that are stitched together in fragmented and ad hoc ways within manufacturers. Cloud systems represent a next wave of networked-based information technology platforms that are undergoing risk-cost-best practice scrutiny. The SM Platform extends the application of cloud services to integration of cloud services to create new functionality.

Security in advanced manufacturing and use of cloud technologies is both complex and sensitive. There are several high-level principles that open the discussion beginning with the recognition of insecurities with the status quo. There is a need to check possible misconceptions about cyber security.

Myth 1: My data is secure as long as it is inside my company.
Some manufacturers still believe they are secure inside their “four walls” and that cloud services are inherently riskier. Jim Davis, Vice Provost of IT at UCLA and CTO of the SMLC, maintains that the security risks inside companies can be high — and sometimes higher precisely because there is a belief that security is sufficient. “If you believe you’re secure,” Davis maintains, “you’ve probably already been hacked.” The focus on defense by perimeter security is misplaced.

Companies should start from the assumption that they could be breached at any time — and focus as much on mitigation and recovery as they do on prevention. Breaches from internal causes, inadvertent or not, are as important as external breaches.

Myth 2: I do not need to know what data I am keeping and what it is being used for.
Detection and mitigation depend on knowing expected patterns of data and being able to set thresholds for detection, which in turn, depend on knowledge of the operation. Cyber risks emerge from not knowing what data is being collected, where it is stored and where it is used. In the physical manufacturing environment, no one would question the need to know where the machines are located and what they are for. Ironically, the same is not always true in the cyber world. Data are assets — and there is a need to know what data are collected, where they are stored and what they are used for.

Myth 3: I am secure because my vendor products are secure.
Vendors often bring products forward that are certified to be secure — and they often are, as long as they are not integrated into a system. Any time two systems are connected, vulnerabilities can arise. Often there are multiple vendor applications that need to be integrated. It is important to ensure that any networked application interfaces are established with good security protocols.

Myth 4: Technology can solve cyber security risks.
Security is not just a technology problem, it is a people, processes and knowledge problem. Breaches tend to be less about technology failure and more about human error. In fact, one of the biggest attack vectors is phishing schemes. The best technology and security policies — whether smart manufacturing or IT security systems in the plant — will not secure companies' critical information assets unless their employees are aware and trained.

Building Security from the Ground Up

One of the security advantages of SM infrastructure is that developers are addressing security risks ***as*** the system is being built and not tacking on security solutions after an IT asset enters the market. As a cloud-based service for integrating cloud services, the SM Platform addresses security and interoperability challenges holistically as part of the basic architecture of the infrastructure. Secondly, SM is objectives-based — meaning that data are collected for a particular objective. This translates into the knowing exactly what data are stored, collected and analyzed. SM also offers new security approaches that are not present in today's ad hoc approaches.

Some of the key new design principles for using SM infrastructure include:

DMZ Zones: A DMZ between the factory operations and the cloud system manages and mediates data transfers in or out of the company. Secure data transfers or reviews are managed between the DMZ and the cloud service. In the event of cyberattack, the DMZ has already by design segmented information and can support mitigation.

Layered Defenses: With cloud-based SM Platform solutions, cyber defenses are embedded at every layer of the system — identity management, data collection, data transfer and validation, data contextualization, validation of physical actions — rather than at the perimeter.

Forensic Analysis: When an anomalous pattern is detected, the supply chain data in the platform also creates a capability to know who transferred what data at what time, enabling a richer forensic analysis.

Detection Mechanisms: The SM Platform supports enterprise modeling and analytics that establish data patterns of expected behavior, including across the supply chain. Sensor patterns of behavior can be established across a supply chain and used to detect abnormal data patterns that can trigger an alert (akin to credit card alerts) in context. Patterns include not only sensor data patterns but also computational patterns. It is possible to also analyze expectations for the various levels of the infrastructure from infrastructure, platform, software and deployment layers of the SM Platform. Individually and together, all of these can be useful for rich security detection.

Authentication and Authorization Data: The SM Platform manages data about who has accessed the data and who is authorized to access the data. This management capability is essential for secure operations normally and is essential for robust detection and mitigation in the event of a security attack.

Rapid Compartmentalization of Infected Devices: In the event a server itself is compromised, cloud-based systems make it possible to quickly isolate and remove tainted servers. This is not as easy or rapid when the software resides on dedicated hardware with a company. Similarly, cloud-based solutions manage validated software images instead of software licenses that are repeatedly compiled.

Final Thoughts

In the final analysis, this fourth industrial revolution will revolutionize not only factory based manufacturing but also supply chain operations, bringing real-time intelligence, optimization, reaction and predictive capabilities to the supply chain. Smart manufacturing turns supply chains into value chains by enabling information exchange not only on cost, quality and delivery, but on product design and manufacturing processes. Information can be exchanged not only with OEMs, but with the entire network of suppliers in the value chain — and that exchange occurs in business real-time, not over days or months.

SM will facilitate far greater interoperability throughout supply chains, but it will require far greater collaboration between IT and operations than exists today. The ability to reap the productivity benefits of a smart value chain will require every supply chain manager to become more engaged in the opportunities and risks in the use of integrated data and the role of IT platform infrastructure that provides the capabilities to integrate in ways not possible and/or accessible before.