MANUFACTURING POLICY INITIATIVE AT SPEA
INSIGHT INTO MANUFACTURING POLICY

Barriers to Smart Manufacturing

Keith B. Belton

Few subjects garner more attention from industry executives than *smart manufacturing*—the integration of sensors, controls, and software platforms to optimize performance at the unit, plant, and supply chain levels. Such integration, facilitated by the Industrial Internet of Things (IIoT), allows for real-time decision making via data analytics, including artificial intelligence (AI).

According to the McKinsey Global Institute, the IIoT can be expected to add between $1.2-3.5 trillion in value in 2025. Consulting firm Capgemini claims that smart factories will enable a 7x increase in overall productivity by 2022, and have the potential to add $500 billion - $1.5 trillion to the global economy within five years. For a typical automotive original equipment manufacturer (OEM), this represents a doubling of operating profit.

These projections are based on a wide array of applications in practice, including predictive maintenance (e.g., networked sensors can pick up subtle changes in equipment that may indicate impending failure), enhanced quality control (e.g., aircraft engine manufacturers can inspect turbofan blades in 3D with micrometer precision), demand-driven production, inventory optimization, reduced energy and material costs, product design (e.g., Airbus has used generative techniques to create aircraft parts that are significantly lighter than those designed by humans) and improved safety and environmental performance.

Smart manufacturing of entire supply chains may be inevitable, but it is not going to arise effortlessly. There are major barriers impeding investment. First, robust processes and devices will not be developed overnight; the needed technologies—such as AI—are evolving. Second, investment cycles in the manufacturing sector are extremely long; complete capital replacement will take decades. Third, the smart manufacturing revolution depends critically on policies impacting the gathering, dissemination, and analysis of data (information governance). Policy choices will shape the future of smart factories.

MPI Roundtable

To explore these information governance issues in some depth, the Manufacturing Policy Initiative at Indiana University hosted an October 19th roundtable event in Washington, DC, featuring executives from nearly twenty manufacturers, each having a global presence. Our goal was to elicit their perspective on the challenges/barriers to smart factories. We invited policy experts to contribute papers on selected topics—AI in manufacturing, technical standards, cybersecurity and privacy, and digital trade policy—to inform and help spur the discussion.

These papers, along with a summary of the roundtable—will be released as an MPI publication in early 2019.

Table 1 highlights the roundtable discussion on these information governance issues.

Table 1. Information Governance issues in Smart Manufacturing.

Topic	*Challenges*	*Possible Solution(s)*
Cybersecurity	Solutions for OT and IT will differ. Small companies represent the weakest link in the supply chain. No single cybersecurity solution can address all vulnerabilities for a firm.	Each firm must choose a unique range of solutions that address the largest share of vulnerabilities. SME vulnerabilities must be minimized. Cybersecurity insurance may drive best practices.
Privacy	No global standard has yet emerged, which hinders investment.	Develop a risk-management-based approach to privacy protection.
Talent	Manufacturing is not perceived to be high tech. Attracting data analytics and AI expertise into manufacturing is difficult.	Improve the perception of manufacturing with those seeking a career in data analytics and AI.
AI	Decisions made with AI cannot be easily audited, and a mistake can be very costly.	AI is most valuable when it provides actionable intelligence.
Technical Standards	SMEs neither engage in standards development nor are early adopters of new standards.	Incentives are needed to drive SME engagement and adoption.
Digital Trade	National governments are creating different rules for the flow of digital information.	Global norms/rules must first emerge.

Cybersecurity. Smart manufacturing won't fulfill its promise without reliable cybersecurity. In our conversation, three themes emerged: First, cybersecurity for operational technology requires a different approach than that for information technology—a distinction not always made by regulators. Second, smaller companies often lag behind larger companies in terms of awareness and adoption of cybersecurity measures, and this hurts all companies in the value chain. Said one executive in the industrial defense supply chain, "I am a big fan of the NIST framework. But small companies are willing to take on more risk than their larger customers. Small and medium enterprises (SMEs) are thus making risk decisions for us." Third, no single cybersecurity solution can address all vulnerabilities in a typical manufacturing environment, making investment decisions difficult. As one executive concluded, “There will always be multiple products to buy. The trick is knowing which few will get you 80% there.”

Privacy. The executives recognized that ensuring privacy of personal information is an active area of policy making that impacts manufacturers, even those that do not sell directly to individual consumers. When suggesting that a company should just adopt the EU General Data Protection Regulation (GDPR) as a global standard, others argued against it. Although strong in certain respects, GDPR is weak in others. And the US is likely to impose its own standard eventually. The National institute of Standards and Technology (NIST) within the US Department of Commerce has just started its year-long effort to develop a risk-based privacy framework building on the success of its cybersecurity framework. Given differences across companies in the manufacturing sector, a risk management approach was seen as the best approach.

Talent. Smart manufacturing will exacerbate the ongoing “skills gap” in manufacturing. This is a big issue for those seeking to attract employees with skills in such fields as data analytics and AI (including machine learning). A big part of the challenge is cultural; parents do not want their children to pursue a career in manufacturing and those seeking a career in data analytics or AI prefer to work for companies in Silicon Valley. Several of the executives acknowledged a need to make manufacturing “cool” to young adults, especially those who do not believe manufacturing is high-tech.

AI. The emerging consensus among the executives was that AI can be useful in some cases, especially if there’s a human overseer. However, the consequences of a failure in a continuous manufacturing process are so severe that executives have a high degree of trepidation of AI and machine learning as a decision maker absent human oversight. As one executive noted, “Actionable insight is what we need from AI.”

Technical Standards. Smart manufacturing cannot be realized without the emergence of global standards to ensure communication along supply chains and provide certainty to investors. Other countries—notably Germany (with Industrie 4.0) and China are aggressively moving to create standards that benefit their domestic industries. Although no one suggested that the US government should prioritize its standard-setting efforts by adopting a top-down approach like that of China or Germany, there was sympathy/support for a more aggressive US posture. The discussion veered toward SMEs, which represent a large share of global value chains. SMEs will need incentives to drive engagement--participating in development and also in adoption of standards. One proposal involves expanding the scope of the R&D tax credit to include firm involvement in standard setting activities.

Trade Policy. Smart factories link digital technologies with production processes. The technologies underpinning smart factories (e.g., 3D printing, IIoT, etc.) will transform trade in manufactured goods. Given this transformation, policymakers should update trade policies and agreements and should develop interoperable norms governing data. However, only two trade agreements, CPTPP and NAFTA 2.0—neither of which is yet in effect—include provisions governing cross-border data flows. Nations are not approaching these issues uniformly. Whereas the US policy is to support a free flow of information across borders, the EU is regulating (restricting the use of) certain types of personal data, and other countries (e.g., China) are restricting the flow of all information (e.g., data localization requirements). Trade disputes have and will continue to arise and be decided before digital trade policy evolves enough to give manufacturers greater certainty.

Meeting Summary

Two clear themes—and questions about the appropriate role of the US government—emerged from the meeting:

Collective action is needed to create information governance conducive to investment. Much of this collective action will or could be initiated by manufacturers themselves, working in coordination with government, or by service providers. For example, the increasing availability of cybersecurity insurance is driving best practices to reduce vulnerabilities. But in some policy areas of import, proactive steps by manufacturers are difficult to recommend. In these cases, governmental action will provide regulatory certainty that drives investment. For example, with respect to trade policy, rules on cross-border data flows will eventually emerge through new trade agreements and the resolution of digital trade disputes.

Policy makers should better understand the needs of manufacturers before proposing specific solutions, Manufacturers have unique characteristics that policy makers ought to be aware of as they try to advance information governance. Specifically, these characteristics include the distinction between IT and OT (which has implications for cybersecurity), the complexity of 21st century value chains (e.g., the need for information flow within and across global value chains), and the capabilities of smaller firms (e.g., to participate in standard setting development and adoption) in relation to OEMs. Public policy must be informed by such considerations or it is likely to fall short of its goals.

Participants raised pertinent questions about the role of the US government: Is the US doing enough to provide the certainty that investors need? Is greater coordination needed among various US government agencies? Does the US need a mid-course assessment of its approach in light of the actions of other leading manufacturing countries (e.g., China, Germany)?

The US government has labeled smart manufacturing as a priority. In October, the White House National Science and Technology Council released its *Strategy for American Leadership in Advanced Manufacturing*. One of its three goals is to develop and transition to new manufacturing technologies by capturing the future of intelligent manufacturing systems. The strategy calls for US leadership in promoting innovation in smart manufacturing technology. But this may not be sufficient. To facilitate timely US investment in new technology, issues of information governance must also be addressed.

Keith B. Belton is the Director of the Manufacturing Policy Initiative at Indiana University in Bloomington, Indiana.

Peer reviewers: Chris Peters, CEO, The Lucrum Group, and Stephen Gold, President and CEO, Manufacturers Alliance for Productivity and Innovation (MAPI)

For further reading:

Belton, Keith. 2018. "What's Stopping the Smart Factory Revolution?" *Industry Week*, June 4.

Capgemini Digital Transformation Institute. 2017. *Smart Factories: How can manufacturers realize the potential of the digital revolution*? Capgemini Consulting.

Frere, Eric; Zureck, Alexander; and Rohrig, Katherina. 2018. “Industrie 4.0 in Germany: The Obstacles regarding Smart Production in the Manufacturing Industry,” Social Science Research Network, posted August 15, 2018.

McKinsey Global Institute. 2015. *The Internet of Things: Mapping the Value beyond the Hype.* McKinsey & Company.

National Science and Technology Council, 2018. *Strategy for American Leadership in Advanced Manufacturing*, Office of Science and Technology Policy, October.

Shackelford, Scott. 2018. “Smart Factories, Dumb Policy? Managing Cybersecurity and Data Privacy Risks in the Industrial Internet of Things,” Social Science Research Network, posted October 14, 2018.