Challenges and Opportunities

Keith B. Belton

Manufacturing firms are not monolithic; they differ significantly in the products they produce, the inputs they employ to make these products, their upstream suppliers and their downstream customers, their relative size (e.g., in terms of employees or annual revenue); and the processes that transform these inputs into finished goods.

Manufacturers also share certain characteristics. Most serve other manufacturers (B2B) as opposed to end-use consumers (B2C); all manage both operations technology (OT) as well as information technology (IT); production assets often last decades prior to replacement; production downtime is extremely costly and to be avoided if possible; supply chains are increasingly complex in terms of the sheer number and locations of suppliers and customers; and rapidly evolving technology increases demand for employees with a new set of skills.

Might these similarities and differences help explain the major challenges and opportunities faced by manufacturers wishing to create and/or invest in smart factories? To find out, the MPI at Indiana University invited executives from eighteen manufacturing firms to Washington, DC to engage in a facilitated discussion on smart manufacturing, with a focus on information governance issues. In preparation for this meeting, the executives (see the Appendix for a list of participants) were given the preceding papers on artificial intelligence, technical standards, cybersecurity/privacy, and digital trade.

During the meeting, held on October 19, 2018, they were briefed by the authors of these papers. They were also briefed by government officials—subject matter experts on governmental activities in the areas of technical standards, cybersecurity and privacy, and digital trade. Armed with this knowledge, the executives engaged in a facilitated discussion centered on two key questions for each of these three topics. (1) Which public policy issues/questions related to this topic are most important to advance smart manufacturing? (2) Apart from public policy issues, which specific steps or actions related to this topic would best advance smart manufacturing?

The remainder of this paper describes the perspective of these executives, gleaned from the facilitated discussion. To ensure an honest and rigorous dialogue, we promised to refrain from attributing particular comments to particular individuals or companies.

Technical Standards

As the Low paper acknowledges, there are hundreds of standards developed or under development that relate to smart manufacturing. Some groups are developing overarching "reference architecture" to conceptualize the needed standards and help direct the efforts of SDOs and others from around the world. But from the perspective of the firm, these efforts present a complicated labyrinth for navigation. As one participant pointed out during the meeting, "We have a series of stovepipes or silos, each with their own standards. How can we best integrate these?"

One common thread to the ensuing conversation related to the role of the US government. The executives acknowledged that the governments of other countries, such as China and Germany, are more engaged in smart manufacturing standards than is the US government, and that these nations are approaching it from a "top-down" perspective, where government convenes the process and directs the action, as opposed to the "bottom-up," market-driven approach that is more typical of how the US government approaches the development of standards, where companies set the priorities for and lead in the development of high priority standards.

The participants did not see the US approach as being clearly superior to that of Germany or China. And the US has some advantages. As one participant noted, "The US situation is not dire. For example, we have great technological expertise." And this expertise provides the US with an advantage in the standard setting process.

One executive noted an advantage to the German approach, "Industrie 4.0 has provided certainty for investors. The US government is not providing such certainty." There was a sense that smart manufacturing investment by manufacturers would be enhanced should clear global standards emerge.

Offered another participant, "The US government should pursue portability of standards by getting other countries to accept/adopt [those developed here.]"

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.

Offered one executive, "Germany and China have a strategic intent to garner competitive advantage. How can the US leverage its strengths (e.g., technological expertise, high quality manufacturing processes and goods, etc.) to obtain a competitive advantage?"

Two participants suggested that manufacturers should join forces and ask NIST to focus US government attention on a specific set of priorities for smart manufacturing standards. As one noted, if industry takes such action, NIST will respond as it has done so in the past with respect to other technologies. Another participant, building off this idea, suggested that industry focus on "somewhat settled" matters, where consensus is most easily attained. Such a cooperative approach could provide a competitive advantage for all of industry, a phenomenon described as "co-opetition". A successful example of co-opetition from the past would be the US approach to the Y2K issue.

A second emerging theme from the discussion was a need to promote not only standards development, but also standards adoption, especially by small and medium enterprises (SMEs). Said one executive, "There is not enough SME representation in standards development. Our large OEMs drive standards." Said another, who works predominantly with small manufacturers, "SMEs need incentives to drive engagement--participating in development and also in adoption of standards." One participant offered a specific incentive—could the current R&D tax credit be used for standards development process? Although the question was not answered, it underscored a sense from the group that incentives are needed to bring small and medium manufacturers to the standards development table.

Cybersecurity and Privacy

Three themes emerged from the conversation on cybersecurity. The first theme is cybersecurity policy for manufacturing must be informed by the distinction between IT and OT. Requirements appropriate for IT are often inappropriate for OT.

Explained one executive, “The priorities for IT and OT are very different. In IT, the priorities are confidentiality, integrity, and availability (i.e., reliability), in that specific order. In OT, the ordered priorities are reversed: availability, integrity, and confidentiality.” Recommendations or requirements for cybersecurity are written for IT may make little sense for OT. Said one executive, OT requires a different approach to cybersecurity than IT.

After learning that proposed legislation in Congress would require patches to limit cyberattacks, another participant pointed out that “patches” are commonly employed in the IT world to limit cyber threats, but this technique would be unacceptable for OT in a manufacturing setting given the priorities of control and availability. In IT, a company can install a patch every week. In OT, a company may want to install a patch every decade—maybe. There must be no slowdowns, no disruptions to the manufacturing process. Other executives acknowledged that the proposed legislation is more suited to B2C than B2B.

A second theme emerging from the conversation was that 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, “I am a big fan of the NIST framework. But small companies are willing to take on more risk than their larger customers. SMEs are thus making risk decisions for us.”

The requirements in the NIST framework, imposed by DoD on its supply chain, proved to be a challenge for smaller businesses. The fact that DoD backed off on enforcement allowed manufacturers to avoid the need to achieve fast and full adoption. One participant noted that without enforcement, people won’t comply. Clarity on the rules is needed. Offered another, “Manufacturers are slow to change. We have a rusty and lazy asset syndrome. We need a drop-dead date for compliance.” Said a third, “Some companies have separated their shop floor from the rest of the company to comply with NIST 1-800-71. This is bad for smart manufacturing.”

One executive opined that US manufacturers are adopting cyber protections more slowly than manufacturers in other countries, perhaps because US supply chains are more diverse due to heavy outsourcing over the last 20 years. It would be a useful area of research to determine if other countries adopting smart manufacturing faster than the USA and, if so, to determine the reasons.

A third theme related to compliance. For example, some noted the difficulty in finding a single solution to ensure cybersecurity and compliance with regulatory requirements in the US and around the world. Lamented one executive, responsible for global cybersecurity, “There is no single product I can buy to get cyber security to where it needs to be." Offered another, "There will always be multiple products to buy. The trick is knowing which few will get you 80% there."

Several observed the difficulty in tracking regulatory requirements for cybersecurity, as requirements are ever-evolving. In response, another participant identified a couple of online resources: the Global Cybersecurity Index, and the Carnegie Endowment Cybersecurity Norms. Others observed that companies are loathe to report cyberattacks, yet such information is necessary as a warning system for others. In response, one participant noted that in recent years, private sector companies in the same line of business have created Information Sharing and Analysis Centers (ISACs), which work well in alerting all within a particular industry to emerging cybersecurity threats.

With respect to privacy, discussion centered on emerging national standards. As one executive said, "Companies want certainty over requirements to protect personal privacy and prefer a global standard over multiple national standards." When suggesting that a company should just adopt GDPR as a global standard, others argued against it because while GDPR is strong in certain aspects, it is weak in others. And because the USA is likely to impose its own standard eventually (e.g., the NIST privacy framework under development) different from GDPR, a long-term reliance on GDPR makes little sense.

Several of the executives agreed that a risk management approach to privacy (underway at NIST) is the right approach given differences across companies in the manufacturing sector.

Digital Trade

Digital trade issues arise when the flow of information relating to smart manufacturing crosses national borders or when policies otherwise impact the flow of information within a nation. For example, consider a heavy piece of equipment, made in the US, that is able to transmit digital information about its activity. If a foreign country restricts the digital information that can be transmitted by this equipment, it will lessen the value of the product while benefitting a competitor product that does not have any digital capability. For manufacturers of "smart" products, the evolution of digital trade rules will have a big impact on their investment.

The executives raised more questions than answers about digital trade policy. There was agreement that digital trade policy will have a big impact on manufacturers, but it is not clear how the international rules will evolve, as pointed out in the Aaronson paper. While the US policy is to support a free flow of information across borders, the EU General Data Protection Regulation (GDPR) represents a different approach, while other countries (e.g., China) are restricting the flow of information much more (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.

Furthermore, the impact of a more certain digital trade policy options are likely to differ across manufacturing firms given the wide variety of circumstances firms face such as the countries in which they operate, their product offerings, and their business model.

One executive asked about data gathered by B2B firms—will the data be considered “personal” or “public” or something else (e.g., confidential business information) covered by trade agreements or local regulation? The question is unknowable today and will only become clearer over time, as trade policy evolves. Another participant said that emerging digital capabilities of medical devices raise critical questions about the data: Who owns it? Who controls it? Such questions should, ideally, be answered before the norms for digital trade policy are established.

Artificial Intelligence

Given the rapid expansion of AI-enabled applications in manufacturing, outlined in the Crandall paper, and the potential for realizing the promise of smart manufacturing, participants of the roundtable engaged in a discussion of its strengths and weaknesses.

The executives readily acknowledged the emerging importance of AI and the difficulty many are having attracting AI expertise into the manufacturing sector. New college graduates with AI expertise, said one participant, are attracted to the tech sector and companies like Google and Amazon and not attracted to enter manufacturing. The common lament was that AI talent is a scarce resource that greatly limits investment in smart manufacturing.

A few of the executives felt that current interest (hype?) in AI is a misplaced. To them, if a company identifies a problem, then maybe AI is an appropriate tool to address it. But acquiring AI expertise and then looking for a problem to solve isn’t productive. To these executives, the appropriate question is not “How can I utilize this cool new technology?” but rather “Can I monetize AI expertise in my business? If so, how?” To these executives, it is not enough to recruit someone with AI expertise, the person must also know enough about the particular business and the manufacturing process to be able to apply it. This makes recruitment even more difficult.

Part of the problem, noted one executive, is cultural; parents do not want their children to pursue a career in manufacturing. Several of the executives acknowledged a need to make manufacturing “cool” to young adults, especially those who do not believe manufacturing is high-tech.

A few of the executives inquired about the ability to audit and understand the rationale for a conclusion reached via machine learning. Upon hearing that AI-enabled conclusions are often impossible or prohibitively costly to understand via audit, the participants in the room turned the discussion toward practical applications.

A few of the executives acknowledged employing AI in their operations. Others acknowledged planning for it in the future. The Crandall paper, which distinguished between situations where AI performs well and situations where it does not, fostered some reflection on the experience of the executives in attendance.

According to one participant, “We use machine learning in specific applications where it can outperform a person. We reject it when it is predictive unless it provides actionable insight. If we cannot understand a result, we do not adopt it.”

Another participant noted that his company uses AI to help identify and then code into a computer why a machine fails. This has replaced a labor-intensive exercise that, too often, was done haphazardly. In this particular application, employing AI improved the accuracy of the coding. And humans still check the AI- coded reason before it is accepted.

A third executive distinguished between AI as a decision-making tool (“it can help humans make decisions”) and AI as a predictive tool. The company is utilizing AI to assist in decision making but sees predictive applications in the future.

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.”

Conclusions

Today, vendors are pitching a myriad of “smart manufacturing” technologies and solutions to a very conservative sector of the economy. To many of the executives at the roundtable, investment in smart manufacturing is akin to placing a huge bet on an uncertain future, which will be shaped by rapidly changing technologies and slowly evolving rules.

Nevertheless, these executives believe that a smart manufacturing evolution is underway and represents a significant transformation of the production process.

Information governance issues associated with smart factories will require collective action to create an environment conducive to investment. Much of this collective action will or could be initiated by manufacturers themselves, working in coordination with government.

To advance information governance, government officials ought to know that manufacturers have certain unique characteristics relevant to policy. These characteristics include distinct priorities associated with IT versus OT, the complexity of 21st century value chains, and the limited capabilities of smaller firms. Information governance for smart manufacturing must be informed by such considerations or it will fall short of its goals.

In some important policy areas such as digital trade policy and privacy policy, proactive steps that manufacturers can take are difficult to identify and recommend. Eventually, a more certain policy environment will emerge, which will allow for more informed smart manufacturing investment decisions.

Peer Reviewers; Stephen Gold, President and CEO, Manufacturers Alliance for Productivity and Innovation; Ward Melhuish, Partner, Grant Thornton; and Timothy Mealey, Cofounder and Senior Partner, Meridian Institute.