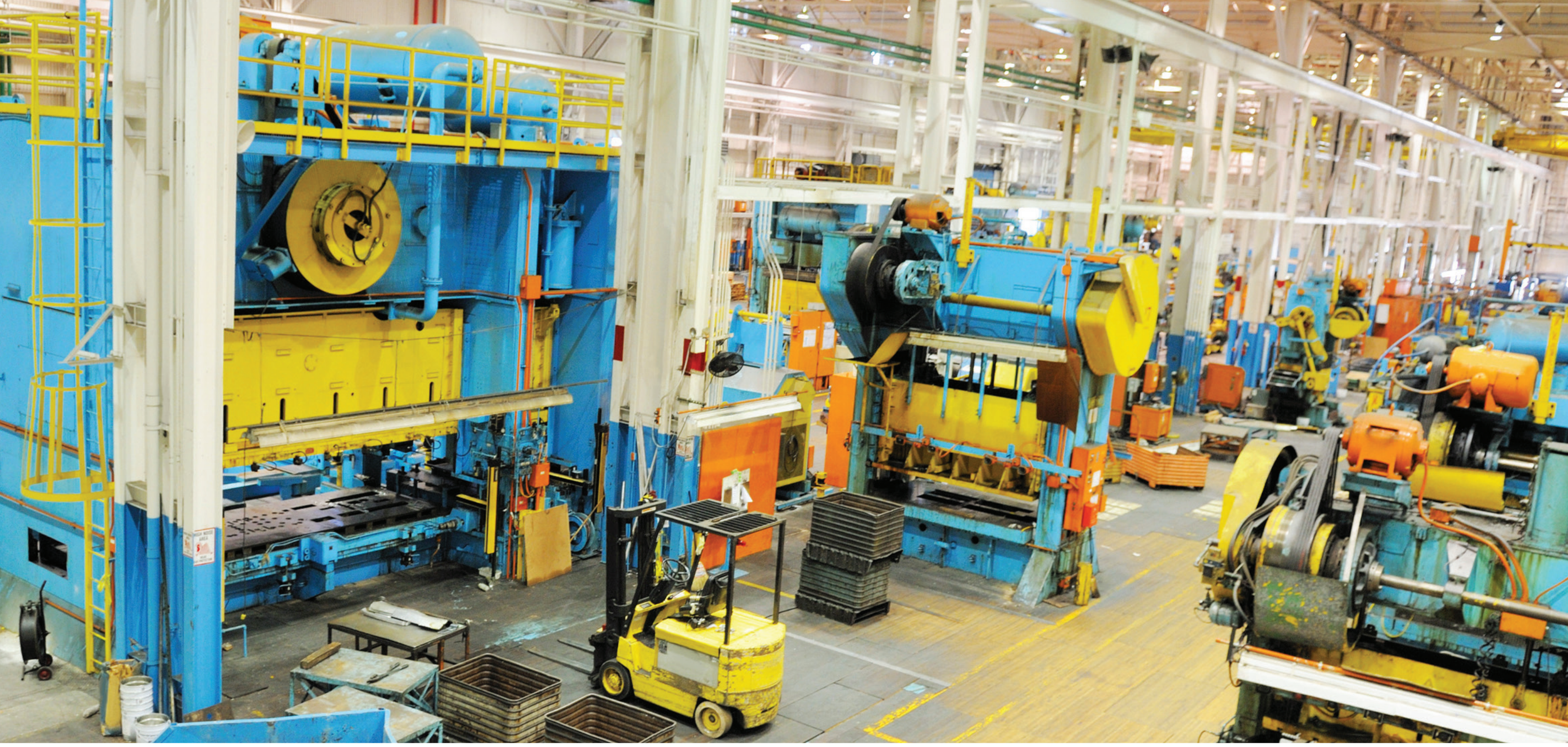


CYBERSECURITY FOR MANUFACTURERS:
Securing the Digitized and Connected Factory

MFORESIGHT
ALLIANCE FOR MANUFACTURING FORESIGHT

CCC
Computing Community Consortium
Catalyst

CYBERSECURITY FOR MANUFACTURERS: SECURING THE DIGITIZED AND CONNECTED FACTORY

KEY TECHNICAL CONTRIBUTOR: PROF. JAMES DAVIS, UCLA
EDITOR: THOMAS MAHONEY, MFORESIGHT

SEPTEMBER 2017
REPORT NUMBER: MF-TR-2017-0202

MForesight: Alliance for Manufacturing Foresight serves as the voice of the national advanced manufacturing community, providing government, academia and industry with information and analysis about emerging technologies, workforce training, and opportunities for public-private partnerships that strengthen U.S. competitiveness. MForesight is funded by the National Science Foundation (NSF) and the National Institute for Standards and Technology (NIST).

The mission of Computing Research Association's **Computing Community Consortium (CCC)** is to catalyze the computing research community and enable the pursuit of innovative, high-impact research. CCC conducts activities that strengthen the research community, articulate compelling research visions, and align those visions with pressing national and global challenges. CCC is funded by the NSF.

This material is based upon work supported by the National Science Foundation under Grant No. 1552534 through a cooperative agreement with the University of Michigan (Dr. Sridhar Kota, Director). Any opinions, findings, conclusions, or recommendations expressed in this material are those of MForesight and do not necessarily reflect the views of the National Science Foundation or the University of Michigan.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyberattacks now regularly make global headlines. While the implications of electronic threats to IT systems, finance, healthcare, and government administration are well-known, there are also very significant and growing—though less well-known—implications for manufacturers. The recent "WannaCry" virus that disabled much of the United Kingdom's National Health Service also forced a Honda plant in Japan to halt production. In June 2017, more than half of the organizations targeted by the Petya (also known as Expetr) cyberattack were industrial companies.

The scale and variety of cyber-threats to manufacturers have grown considerably in recent years, and now range from rare and sophisticated Stuxnet-style attacks to relatively frequent ransomware risks. In addition to malware attacks on industrial firms, cyberattacks on manufacturers can include efforts to corrupt data, steal intellectual property (IP), sabotage equipment, and disable networks. The purposes and effects of attacks vary widely, but all such incidents cost time and money to industrial firms and their customers.

As manufacturing becomes increasingly digitized and data-driven, manufacturers will find themselves at serious risk. Although there has yet to be a major successful cyberattack on a U.S. manufacturing operation, threats continue to rise. The complexities of multi-organizational dependencies and data-management in modern supply chains mean that vulnerabilities are multiplying.

There is widespread agreement among manufacturers, government agencies, cybersecurity firms, and leading academic computer science departments that U.S. industrial firms are doing too little to address these looming challenges. Unfortunately, manufacturers in general do not see themselves to be at particular risk. **This lack of recognition of the threat may represent the greatest risk of cybersecurity failure for manufacturers.** Public and private stakeholders must act before a significant attack on U.S. manufacturers provides a wake-up call.

Cybersecurity for the manufacturing supply chain is a particularly serious need. Manufacturing supply chains are connected, integrated, and interdependent; security of the entire supply chain depends on security at the local factory level. Increasing digitization in manufacturing—especially with the rise of Digital Manufacturing, Smart Manufacturing, the Smart Factory, and Industry 4.0, combined with broader market trends such as the Internet of Things (IoT)—exponentially increases connectedness. At the same time, the diversity of manufacturers—from large, sophisticated corporations to small job shops—creates weakest-link vulnerabilities that can be addressed most effectively by public-private partnerships.

These vulnerabilities are particularly concerning in the large, complex supply chains for weapons systems and other manufacturing procurement by the Department of Defense (DoD). **The consequences of a cyberattack on defense production could be profound,** possibly limiting production volumes and schedules, as well as having the potential for catastrophic failure of weapons systems and equipment.

Experts consulted in the development of this report called for more holistic thinking in industrial cybersecurity: improvements to technologies, management practices, workforce training, and learning processes that span units and supply chains. Solving the emerging security challenges will require commitment to continuous improvement, as well as investments in research and development (R&D) and threat-awareness initiatives. This holistic thinking should be applied across interoperating units and supply chains.

Much like quality systems, cybersecurity improvements should ideally be market-driven, and based on quantified insurance risk or competitive financial advantage. Still, more extensive government regulation may be needed, mirroring industrial safety and health. Regardless of the form that these changes take, it is clear that new risk management and opportunity models are needed to address the rise of hyper-connected, multi-vendor hardware and software platforms. Stakeholders across sectors must work together to build a culture of vigilance and to apply essential security practices across supply chains.

Cooperation is key. **There is a critical need for industry-government-academia cooperation to build the collaborative components of a supply chain/ecosystem security framework.** Multiple government programs are now engaged in this work, including the DoD, Department of Energy (DoE), Department of Commerce (DoC), Department of Homeland Security (DHS), the National Science Foundation (NSF), and the National Institute of Standards and Technology (NIST). The Manufacturing USA institutes and Hollings Manufacturing Extension Partnership (MEP) program have important roles in testing, training, and technology implementation. Academic programs, such as those at Texas A&M University and the Virginia Polytechnic Institute and State University, as well as key vendors in cybersecurity research and training, must be involved in development, dissemination, and implementation of effective cybersecurity solutions. A great deal of existing capability can be focused on manufacturing, but R&D to create effective technologies and new capabilities is needed to achieve a truly cyber-secure manufacturing sector. A holistic approach to cybersecurity requires support from diverse players across sectors.

SUMMARY OF RECOMMENDATIONS

Within the overall context of the cybersecurity challenges facing manufacturers, workshop participants and contributors recommend the following areas of action to achieve both near and long-term benefits:

1. Create a public-private partnership focused on manufacturing supply chain cybersecurity. Specific tasks for such a partnership include:

   a. Develop a national strategy for strengthening manufacturing cybersecurity that would identify and coordinate existing public and private efforts as well as additional resources sufficient to address the diverse testing, training, and R&D needed to meet the challenges in manufacturing cybersecurity.

   b. Accelerate the application of existing cybersecurity technologies and practices to manufacturing to immediately lower the risks of cyberattacks.

   c. Coordinate facilities and mechanisms to address R&D challenges identified in Recommendation 2.

   d. Support manufacturing sector specific Information Sharing and Analysis Centers (ISACs)/Information Sharing and Analysis Organizations (ISAOs) (Recommendation 3).

   e. Coordinate cyber ranges and test beds to

      i. ensure comprehensive testing for vulnerabilities and effective patching in components, equipment, software, and other aspects of networked cyber physical systems (CPS) of systems,

      ii. act as sandboxes to test new ideas safely and securely,

      iii. provide "cyber autopsy" capabilities, and

      iv. promote the creation of standard models for Operations Technology (OT) systems.

   f. Coordinate the development of curricula and creation of boot camps for effective training of the general manufacturing workforce in cybersecurity best practices, as well as OT and Information Technology (IT) technical professionals in evolving threats, emerging technological solutions, effective OT/IT interface, and CPS of systems engineering.

2. Establish a federal research initiative to address both near- and long-term cybersecurity challenges and opportunities. Fundamental research should address systems of systems engineering methodologies for cyber physical systems with designed-in cybersecurity and resilience, treating linked cyber spaces as systems design/interface risk problems. Critical development activities that should commence now and require support to evolve include:

   a. Create systems and security reference architectures for manufacturing that define the OT and IT functions, standards, and integration requirements. The reference architectures should be applicable across a diverse range of manufacturing devices, operations, and enterprises, and different vendor control, modeling, and automation platforms.

b. Establish software and hardware trust anchor frameworks for securely connecting and managing many devices, systems, and data in manufacturing systems without central management.

c. Develop systems-of-systems architecture design and analysis that include integration with cloud services.

Critical R&D objectives that would benefit from immediate focused attention include creation of:

a. Automated vulnerability assessment and detection tools. Many tools currently exist but are not tuned for manufacturing or the operational requirements of a production setting.

b. Analytics-based detection—networks or machines—and use of digital twins.

c. Tools to audit the extent of attacks.

d. Automated, robust part validation technology, including automated ledger technologies such as blockchain, for trusted parts and data validation.

3. Establish manufacturing industry-specific ISACs/ISAOs or similar organizations to facilitate fault-free, anonymous sharing of incidents, threats, vulnerabilities, best practices, and solutions. Existing ISACs/ISAOs provide models. Proactive collaborative activities that manufacturing-specific ISACs/ISAOs could initiate include:

a. Develop a data repository of anonymous submissions of cyberattacks, and disseminate anonymized reports to manufacturers on a regular schedule.

b. Coordinate use of decoys for intelligence gathering and sharing.

c. Create industry test beds, cyber ranges, and demonstration facilities to safely prototype and test OT and IT security technologies, identify system-level vulnerabilities, and provide a “cyber autopsy” capability.

d. Identify and disseminate best practices and provide training platforms/curricula.

4. Establish an executive-level working group to provide a strong industry voice to advocate for and motivate industry action to strengthen cybersecurity. Using the emergence of quality system certifications as a model, the working group should drive market-based incentives for stronger cybersecurity in manufacturing. The goal should be for most manufacturers to implement the practices identified in the Repeatable and Adaptive Implementation Tiers in the NIST Cybersecurity Framework, and to meet the requirements in relevant standards such as ISA/IEC 62443 and ISO 27001. Certification to those standards should become a requirement for purchasing decisions, similar to ISO 9001. The working group should also:

a. Promote participation by all manufacturers in their industry’s ISAC/ISAO.

b. Facilitate the emergence of financial risk management procedures that can apply to cybersecurity practices.

c. Communicate with executives in other at-risk economic sectors such as finance and energy to ensure that solutions developed for those industries are applied in manufacturing.

5. Similar to existing frameworks on cybersecurity and cyber physical security, a comprehensive framework should be developed specifically for manufacturing supply chain cybersecurity. It should reference:

a. robust part validation technologies,

b. methods to audit attacks and responses,

c. a common language across multiple functional departments and organizations, and

d. application of appropriate standards such as ISA/IEC 62443 and ISO 27001.

ABOUT THIS REPORT

On March 14-15, 2017, MForesight, in cooperation with the Computing Community Consortium, convened a workshop of manufacturing and cybersecurity experts to address the unique and complex cybersecurity issues facing manufacturing as the digitization of the industry grows. The goals of the workshop were to:

1. Consider useful steps to accelerate adoption of cybersecurity practices across manufacturing supply chains that depend on interdependency and interoperability of individual company practices;
2. Identify priority activities to raise awareness and implementation of cybersecurity technology and management practices to achieve inherently secure, repeatable, and adaptable manufacturing activities; and
3. Align next-generation cybersecurity research with the needs of manufacturers.

The workshop outcomes were enhanced by subsequent discussions with other experts in specific cybersecurity areas. This report summarizes the consensus of these manufacturing, government, academic, and coalition experts focused on cybersecurity in manufacturing. (See Appendix 3 for a list of contributors and Appendix 4 for the workshop agenda.)

CHAPTER 1

INTRODUCTION: THREATS TO CYBER PHYSICAL SYSTEMS

Cyberattacks pose a growing threat not only to national security but also to U.S. economic competitiveness. Manufacturing firms, in particular, are vulnerable to threats including sabotage of operations, alteration of data and product designs, and theft of intellectual property.

Cybersecurity for manufacturing requires serious attention. The sector presents special security challenges because of the unique nature of cyber physical systems (CPS), which includes operations technology (OT) such as industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and networked machines, sensors, data, and software.[1] Changes to these systems can result in physical changes in materials, parts, and environments. Effective response to cyberattacks on manufacturing firms requires a critical assessment of gaps in the technology, broad adoption of existing best practices, and research to develop inherently safe systems and rapid response tools. Cybersecurity measures must be enhanced to protect a

[1] Appendix 2 provides a glossary of terms commonly used in manufacturing technology and cybersecurity.

highly integrated and interoperable network of manufacturers and service providers.

To date, the private sector has not adequately addressed the unique cyber threats facing manufacturing firms. **Existing cybersecurity products and solutions designed to secure information technology (IT) systems do not address the cyber threats that target an interconnected system of suppliers and customers.** For example, insecure networks at lower tier suppliers offer entry points for malicious software, which can then infect the entire supply chain. Unfortunately, small and medium-sized manufacturers (SMMs) often do not have the resources to hire dedicated security staff to establish security procedures, adopt standards, and monitor network integrity. Standards relevant to ICS security, such as ISA/IEC 62443 and ISO 27001 (see Appendix 1), provide a starting point, but in the rapidly changing cyber threat environment, their implementation and adoption by manufacturing firms (especially SMMs) has been slow and difficult.[2] Government agencies that support research efforts in cyber physical security offer a range of resources to assist companies in assessing their vulnerabilities,[3,4] but the focus is largely on ICS, and it is often challenging for smaller manufacturers to implement the recommended protection protocols. The academic community has been engaged in developing cybersecurity tools for manufacturing,[5,6] but the breadth of risks and implementation challenges leave many manufacturers vulnerable.

The unauthorized access and control of digitally controlled systems is of particular concern in the manufacturing community. In contrast to conventional IT systems, cybersecurity of manufacturing poses a unique challenge to CPS. **Every manufacturing job introduces new executable code into these systems, making the data flowing through the system vulnerable to theft and/or alteration.** According to the 2015 White House Supply Chain Innovation Initiative (2015), standards related to cybersecurity are particularly challenging, as original equipment manufacturers (OEMs) are increasingly demanding minimal digital safeguards to maximize interoperability throughout their supply chains. As software-based control and monitoring of manufacturing machines increases, the risk of malicious cyberattacks also grows.

CYBER THREATS TO U.S. MANUFACTURING

Manufacturers, particularly those in critical manufacturing industries, have long been recognized as potential targets of cyberattacks. Attacker motivations span a broad range including theft of intellectual property (IP) and trade secrets, sabotage of processes and output, extortion, and malicious damage to networks and information systems. Recent patterns of cyberattacks confirm that, although financial services, public administration, and utilities are the most targeted economic sectors, manufacturing is a significant target. Within manufacturing, the automotive, chemicals, and computers and electronics industries are targeted most frequently (see Figure 1).

[2] NDIA White Paper: Cybersecurity for Manufacturing, May 2014.

[3] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/ FY2015_Industrial_Control_Systems_ Assessment_Summary_Report_S508C.pdf.

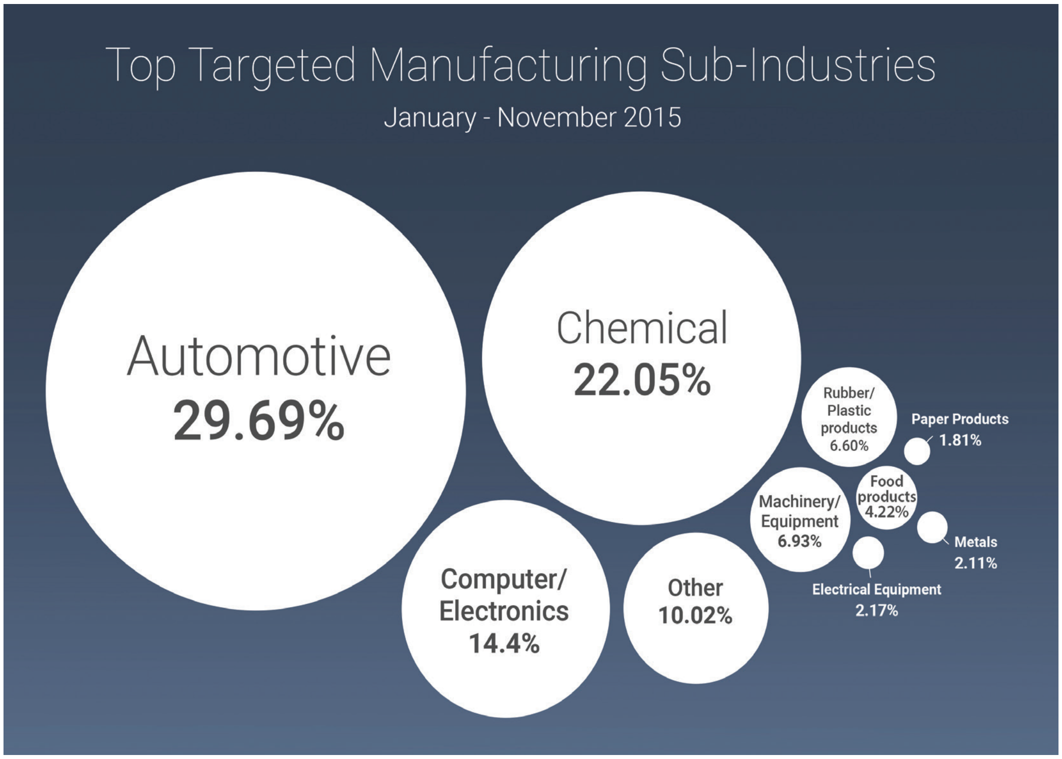
[4] https://ics-cert.us-cert.gov/Assessments.

[5] https://cybersecurity.tamu.edu/about-us/.

[6] https://sites.google.com/a/vt.edu/cyber-physicalsecuritysystemsmfg/.

FIGURE 1. TOP TARGETED MANUFACTURING SUB-INDUSTRIES.

SOURCE: IBM MANAGED SECURITY SERVICES.



Cybersecurity firms such as Kaspersky, McAfee, Trend Micro, and Symantec track the sources and types of threats, their objectives, and their targets as they change over time. In general, the number of reported so-called zero-day vulnerabilities, that is, a vulnerability in software that is unknown to the vendor, declined by approximately 20 percent from 2014 to 2016.[7] For systems important to manufacturers, the number of vulnerabilities discovered in ICS fell in 2016 to 165, down from 200 in 2015 (see Figure 2).[8] New vulnerabilities were discovered in 2016 in 16 different SCADA applications from 15 different vendors.[9]

As these vulnerabilities are closed, attackers have shifted strategies to use malware attached to email and hidden in legitimate administrative tools to gain access to targeted systems. **Specific to the manufacturing industry, 1 in 130 emails contained malware, roughly equal to the average across all industries, but the number of phishing emails targeting manufacturers was 1 in 3,171, significantly higher than the average.**[10] One type of email attack becoming more popular because of its profitability is called a Business Email Compromise (BEC). In a BEC scam, a spoofed email appearing to come from the company's senior management is sent to a company's financial staff with instructions to transfer funds to the attacker's account. In other cases, the BEC email contains a false or altered invoice. According to Symantec, **more than 400 businesses were**

[7] Symantec, *Internet Security Threat Report,* April 2017, p. 14.

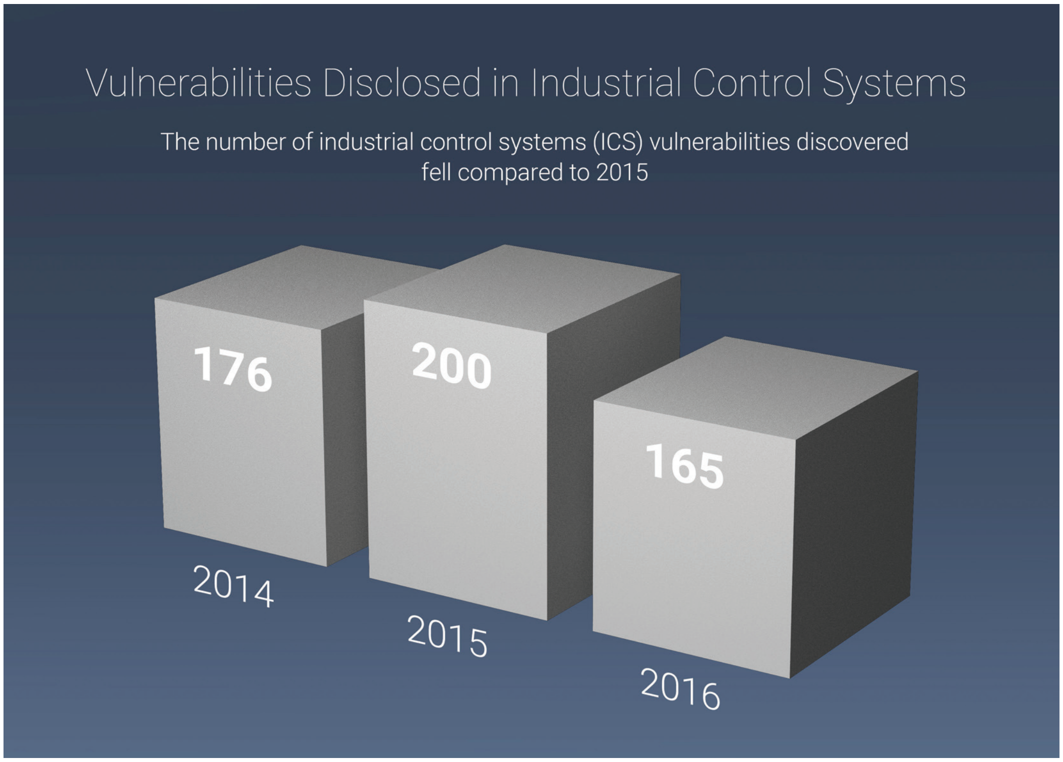
[8] Symantec, p. 17.

[9] Trend Micro, *TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats,* 2017, p. 31 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup.

[10] Ibid., p. 26.

FIGURE 2. VULNERABILITIES DISCLOSED IN INDUSTRIAL CONTROL SYSTEMS.

SOURCE: SYMANTEC, INTERNET SECURITY THREAT REPORT, APRIL 2017.



targeted every day in 2016, resulting in more than $3 billion in losses. In 2016, an Austrian aerospace company lost nearly $50 million in a BEC scam.[11]

Manufacturers also have been the targets of cyber-espionage attacks. **Symantec's research indicates that a majority of cyber-espionage attacks from 2011 to 2013 sought access to IP and trade secrets of manufacturers.** More than half of successful IP thefts involved state-affiliated actors, and 57 percent of these attacks originated in China. However, in 2015, China and the United States reached an agreement in which neither government would conduct or support cyber-enabled theft of IP.[12]

Since then, detections of malware linked to Chinese cyber-espionage groups have fallen significantly, although the threat has not been eliminated.[13] For instance, in July 2016 a Chinese cyber-espionage group targeted defense industries in Russia, Belarus, and Mongolia. In the same month, a new strain of cyber-espionage malware targeting European energy companies was discovered.[14]

Another type of attack targeting manufacturers seeks to alter automated production processes with the intent of destroying the production equipment or compromising it enough that output is unusable. Sometimes known as cyber-sabotage, this type of cyberattack is most famously illustrated by the

[11] Ibid.

[12] E. Nakashima and S. Mufson, "U.S., China Vow Not to Engage in Economic Cyber Espionage," *The Washington Post*, September 25, 2015, at https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html?utm_term=.4a1b98dbfaab.

[13] Symantec, p. 20.

[14] Center for Strategic & International Studies, "Significant Cyber Incidents Since 2006," at https://www.csis.org/programs/technology-policy-program/cybersecurity/other-projects-cybersecurity/ significant-cyber.

Stuxnet computer worm targeting ICS in Iran's nuclear facility in 2010. Since then, variants of Stuxnet have been found in the wild, notably the Duqu Trojan found in Europe, that was designed to gather information about ICS,[15] and another variant discovered in 2010 that exploited a Microsoft Windows vulnerability to attack SCADA systems.[16] This worm caused the destruction of a water pump at a public utility in Springfield, Illinois, in 2011.[17] In 2014, malware known as Havex and BlackEnergy took advantage of a flaw in Windows to control SCADA systems.[18] More recently, in 2016, security researchers discovered another Stuxnet variant, called Irongate, designed to target ICS and SCADA systems.[19] Another sophisticated malware that is not a Stuxnet variant was uncovered in June 2017. Known as Crash Override or Industroyer, it was likely used in a cyberattack against the power grid in Ukraine in December 2016. With small modifications, it could be used against electric utilities and industrial targets in the United States.[20] According to one report, attacks on SCADA systems increased by 636 percent from 2012 to 2014.[21] The trend continued in 2016 with attacks targeting ICS more than doubling the number in 2015.[22]

Because of the large number, variety, and complexity of manufacturing control systems, and the high dollar value of lost production, manufacturers, especially SMMs, are ripe for ransomware attacks. The number of ransomware families more than tripled, the number of infections increased 36 percent, and the average ransom amount nearly tripled in the past year, with email serving as the primary attack channel.[23] Among the 247 new ransomware families added in 2016, 70 targeted computer-aided design (CAD) files widely used in manufacturing.[24]

Anecdotal evidence suggests that state-sponsored attacks have tended to target infrastructure grids such as power and water and large critical manufacturing operations. In contrast, attacks on general manufacturers have tended to originate from a diverse set of hackers. **Reported attacks have not been sufficient in number or prominence to motivate much action among manufacturers, even though U.S. manufacturers are the target of nearly half the known cyberattacks on manufacturing (see Figure 3).**

A cyberattack also can come from a host of non-technical sources. A recent study by Deloitte and MAPI[25] found that errors by employees (or deliberate acts) pose a significant concern to companies, especially those firms that are not actively protecting their IP and do not have procedures to protect against insider threats. Many firms falsely think that separating their internal networks and control systems from the external internet (air-gapping) is the most cost-effective cybersecurity strategy, but this approach puts

15 "Stuxnet Variant Discovered in European Systems," *Power,* Oct. 19, 2011, at http://www.powermag.com/stuxnet-variant-discovered-in-european-systems/.

16 J. Kirk, "Second variant of Stuxnet worm strikes," *InfoWorld,* July 20, 2010, at http://www.infoworld.com/ article/2625596/endpoint-protection/second-variant-of-stuxnet-worm-strikes.html.

17 M. Long, "Stuxnet Strike on U.S. Utility Signals Disturbing Trend," *Yahoo News,* Nov. 21, 2011, at https://www.yahoo.com/news/stuxnet-strike-u-utility-signals-disturbing-trend-224036723.html.

18 IBM Managed Security Services, *Security Attacks on Industrial Control Systems: How Technology Advances Create Risks for Industrial Organizations,* Oct. 2015, p. 5, at https://www.ibm.com/marketing/iwm/dre/signup?source=mrs-form-4573&S_PKG=ov39538.

19 M. Kumar, "Irongate—New Stuxnet-like Malware Targets Industrial Control Systems," *The Hacker News,* June 4, 2016, at http://thehackernews.com/2016/06/irongate-stuxnet-malware.html.

20 J. Finkle, "Security firms warn of new cyber threat to electric grid," *Reuters,* June 12, 2017, at http://www.reuters.com/article/us-cyber-attack-utilities-idUSKBN1931EG.

21 IBM Managed Security Systems, p. 5.

22 D. McMillen, "Attacks Targeting Industrial Control Systems Up 110 Percent," *Security Intelligence,* at https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent.

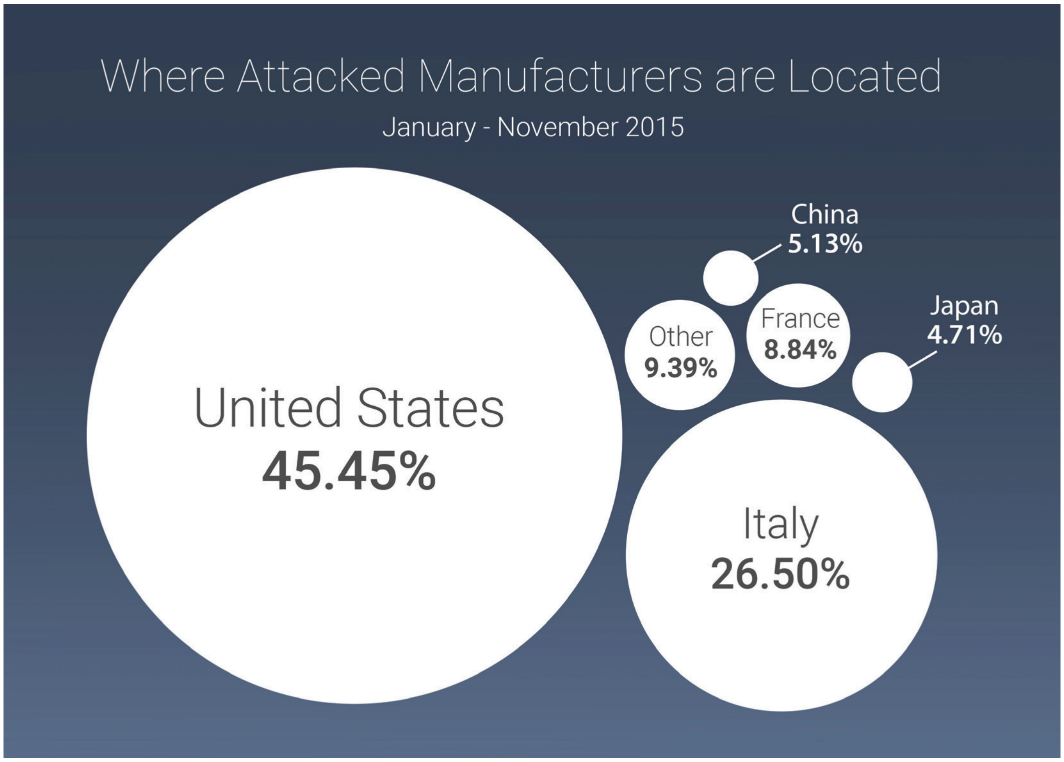
23 Symantec, p. 11.

24 Trend Micro, p. 5.

25 https://www.mapi.net/forecasts-data/cyber-risk-advanced-manufacturing.

FIGURE 3. WHERE ATTACKED MANUFACTURERS WERE LOCATED IN 2015.

SOURCE: IBM MANAGED SECURITY SERVICES



the company at a disadvantage in an increasingly connected world, and is completely ineffective at preventing insider attacks.

The growing digitization of manufacturing production and increasingly complex IT networks within and between factories introduces a growing number of potential vulnerabilities. Meanwhile, the profile of cybersecurity threats is constantly changing as vulnerabilities in software and firmware systems are closed, telltale signatures of malware are recognized, and law enforcement focuses on hacker groups.

Vendors of ICS, SCADA systems, and other cyber system OT and IT components, (e.g., sensors, data connectors, structure and management systems, platforms, analytics and modeling packages, visualization and virtual reality tools) are including cybersecurity features in their product offerings. For example, Rockwell Automation offers products to control access to industrial equipment, detect tampering, and secure factory networks.[26] Global manufacturers GE and Siemens have introduced new operating platforms that promise stronger cybersecurity. GE's cloud-based Predix platform includes data analytics, connectivity, and cybersecurity features.[27] Siemens has introduced a similar platform called MindSphere. Both companies offer internally developed apps and hope to build large communities of independent app developers. Both also offer digital twins: GE has a growing library of virtual digital profiles of more than 500,000 industrial machines; Siemens provides

[26] Rockwell Automation, "Industrial Security: Protecting Networks and Facilities Against a Fast-changing Threat Landscape," July 2016, at http://literature.rockwellautomation.com/idc/groups/literature/ documents/wp/secur-wp004_-en-e.pdf?event-category=eBook&event-action=Download&event-label=Security_Global_XX_EN_2016_Industrial_Security_Whitepaper.

[27] N. Schwiters and B. Moritz, "10 Principles for Leading the Next Industrial Revolution," *Strategy + Business,* March 23, 2017, at https://www.strategy-business.com/article/10-Principles-for-Leading-the-Next-Industrial-Revolution?gko=f73d3.

digital twins to duplicate and simulate products, production lines, processes, and entire factories.[28]

Even as vendors recognize the importance of cybersecurity in their new product offerings, manufacturers operate with a large base and immense variety of old but still serviceable equipment (so-called legacy systems). **The average age of information processing equipment used in manufacturing is 5 years, while conversely, the average age of industrial equipment in 2016 was 10 years, the highest since 1940.**[29] This broad lifecycle diversity poses an enormous challenge: how can risks to legacy systems be assessed appropriately and addressed effectively?

The cybersecurity threats facing U.S. manufacturers are already severe. Digitized, networked, and global supply chains create an extremely complex environment that is difficult, perhaps impossible, to secure completely. The risk to large supply chains in defense procurement is especially concerning given the need to maximize quality and integrity of weapons systems, in which failure of a small fastener in an aircraft, for example, can result in catastrophe. Strong initiatives are needed now in R&D, data sharing and analysis, testing, training, and implementation of solutions. **No single company or single security product can accomplish the steps necessary to strengthen cybersecurity in manufacturing.** Mechanisms for intra- and inter-industry collaboration will be needed. Threats change constantly. Effective action is overdue.

[28] Siemens, "Industrie 4.0: Siemens Demonstrates Digital Twin in Actual Operation," April 24, 2017, at https://www.siemens.com/press/PR2017040272DFEN.

[29] T. Aeppel, "Old Machines Show Why Trump Tax Breaks May Not Spark New Company Spending," *Reuters,* May 19, 2017, at http://www.reuters.com/article/us-usa-manufacturing-investment-analysis-idUSKCN18E1DI.

CHAPTER 2

CREATE A PUBLIC-PRIVATE PARTNERSHIP FOCUSED ON MANUFACTURING CYBERSECURITY

MANUFACTURING CYBERSECURITY CHALLENGES ARE UNIQUE

The very nature of manufacturing creates cybersecurity challenges that other industries do not face, or not with the same risk. More than most industries, modern manufacturing depends on the flow of materials, parts, assemblies, energy, data, and people from many different sources. Cyber physical security must address multiple factories in the supply chain, along with the movement of inputs and outputs that introduce risk, uncertainty, and control challenges. Qualification of all suppliers in the chain is necessary in product specifications, chain of custody, process conditions, and data integrity and security. Securing this complex interaction of potentially vulnerable systems affects all industries, but is especially important in defense production where national security depends on high-quality, reliable weapons systems.

Manufacturing interoperates with key infrastructures that include energy grids, water resources, gas and fuel networks, and a myriad of transportation and distribution systems. All of these infrastructure systems have cybersecurity issues that can affect manufacturing. In this context, infrastructure and service providers such as utilities, gas and fuel systems, and waste treatment facilities are all part of the manufacturing supply chain.

The sequential nature of manufacturing operations exacerbates the challenges. The performance of the next operation depends on high-quality output from the previous operation and may amplify minor changes that can lead to catastrophic effects. For example, minor changes to part definition data can be virtually undetectable yet lead to part failure that can ruin a final assembly or worse, resulting in operational failure.

Factories are always operating, complicating OT and IT maintenance. Checking software versions, installing patches, and performing vulnerability testing are difficult or not possible during operation. A typical factory's aggregate CPS of systems is sufficiently complex (and expensive) that having a separate system to test updates before applying them to the production system is usually not possible. Furthermore, testing during scheduled maintenance downtimes may be impractical and can introduce uncertainty during the restart.

Factory operations are constantly changed and optimized to ensure that product specifications and operational economics, impacts, and safety goals are all met. CPS security must be accomplished in the face of constantly changing conditions that are often stochastic in nature. Furthermore, statistical sampling used to verify manufacturing results are built on top of the stochastic properties of physical manufacturing. Cyberattacks can take advantage of statistical process control (SPC) methods and systems to make detection of quality problems more difficult.

In most factories, the aggregate CPS of systems is a complex mix of equipment and networks from multiple vendors with multiple operating systems, controllers, and interconnections. New equipment works alongside legacy equipment that can be decades old. Equipment from different vendors is typically compartmentalized, requiring third-party software to interconnect proprietary systems. Further, these interconnections are often made in an ad hoc, peer-to-peer manner resulting in a diverse set of non-standard interconnections. Some experts argue that this diversity creates additional challenges for potential hackers that mitigate cyberattack risk. The prevailing consensus, however, is that ad hoc interconnections increase cyberattack risk because they are difficult and costly to maintain for security and operations.

Inherent in the context of systems of OT and IT systems and adding to the complexity, **factories use complex heterogeneous data and modeling systems** spanning a wide spectrum of time constants. Sensor input from and control signals to many different physical assets on very short time frequencies (e.g., millisecond control signals to multiple valves from a Distributed Control System) are common. The latency of the input and/or control signal cannot exceed the control system design parameters, which puts constraints on security measures: cybersecurity measures cannot introduce time lags between sensing and actuation without compromising equipment performance and even operational safety. More generally, the impact of CPS on the physical world and its increasing interconnectedness raise concerns about trustworthiness. Manufacturers at all levels in networked supply chains need to trust that their data, equipment, and systems are safe, reliable, private, and secure.

Cyber physical system security is not just about protecting operations. IP is embodied in product design and associated process design and specifications. The parameters and process specifications that ensure cost-effective production are often highly valued trade secrets that must be protected from hackers.

Finally, to further complicate these inherent challenges, the **prevailing organizational**

structure in manufacturing separates IT and OT. Responsibility for security tends to be within the IT department, tends to focus only on IT, and stops at network security. CPS risk assessments, if done at all, are performed by manufacturing OT groups.[30] Operations rarely consider cybersecurity threats. A rapid increase in recent years in malware targeting industrial control systems, often brute-force attacks on SCADA systems, emphasizes the increasing risks of complacency.

TESTING FOR VULNERABILITIES AND EFFECTIVE SOLUTIONS

One of the greatest challenges to manufacturing cybersecurity is the difficulty of safely testing manufacturing systems. Many security issues arise at the interfaces of interoperable components, often sourced from different manufacturers. Whereas the National Highway Traffic Safety Administration and the National Security Test Site have end-to-end facilities for testing the crashworthiness of vehicles and the survivability of systems, respectively, there is no analogue for cybersecurity in manufacturing. Large OEMs have the means to create entire test factory floors, but even such facilities face challenges to achieving reasonable cybersecurity assurance of the interoperable components in a realistic environment. The ideal solution is a network of test bed and cyber range facilities that share information and findings specifically designed for manufacturing cybersecurity needs.

The federal government can play a vital role in supporting and coordinating testing infrastructures that span multiple stakeholders. For example, Sandia National Laboratory operates the National SCADA Test Bed. Its focus is on energy system reliability, but it has significant overlap with SCADA systems used in manufacturing.[31] The National Institute of Standards and Technology (NIST) has created a small test bed for ICS cybersecurity.[32] The Digital Manufacturing Design and Innovation Institute (DMDII) in Chicago, one of the Manufacturing USA institutes, is in the process of developing an interactive, open cybersecurity test bed that leverages its existing 24,000 square foot manufacturing floor, which contains computer numerical controlled (CNC) machines, assembly stations, a metrology lab, and numerous digital technologies. The vision of the DMDII cybersecurity test bed is to demonstrate recommended cyber hygiene practices, identify and share vulnerabilities, and create a neutral environment to disseminate learnings transparently across the manufacturing community.

In addition to improving the cybersecurity of IT and OT through technical measures, test beds also offer an opportunity for training on these systems. For example, Idaho National Laboratory's Control Systems Analysis Center contains a control system environment specifically configured for an ICS cybersecurity training course. The course includes hands-on training and Red Team/Blue Team training in attacking and defending operations of batch plants and an electrical distribution SCADA system.[33] By engaging researchers from academia and industry, as well as students, more individuals can be exposed to important cybersecurity problems.

Test beds also promote the creation of standard modes for OT systems. **The manufacturing community needs a "lighthouse" for how to build a factory with cyber designed into its DNA; test beds can facilitate this development.**

[30] Aon, *2017 Global Risk Management Survey,* at http://www.aon.com/2017-global-risk-management-survey/index.html.
[31] http://energy.sandia.gov/energy/ssrei/gridmod/cyber-security-for-electric-infrastructure/scada-systems/.
[32] https://www.nist.gov/publications/cybersecurity-test bed-industrial-control-systems.
[33] Details on the training offered are available at https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT.

Manufacturers would also benefit from the establishment of cyber ranges for testing components and system-level vulnerabilities, training teams, acting as sandboxes for new ideas, and providing a "cyber autopsy" capability. Manufacturing-specific IT/OT cyber ranges will create greater opportunities to test manufacturing systems and will increase the capability of internal Red Teams to discover flaws.

WORKFORCE TRAINING

Although programs such as the National Initiative for Cybersecurity Education led by NIST (see Appendix 1) are helping to increase the skills and availability of cybersecurity professionals, **manufacturing companies need workforce training programs/content to increase awareness of best practices without ambiguity and to avoid human error, the highest risk factor.** Additional training needs to be available for existing OT and IT staff to instill consistent, unambiguous security methods and to expand knowledge of and access to available resources. Currently, IT and OT people do not communicate well, nor do IT and Human Resources/Safety staff, because of a language mismatch and competing priorities. There is immense value in creating baseline information and guidance on best practices in cybersecurity as outlined in the NIST Cybersecurity Framework and related documents, how cybersecurity standards and resources are related, the circumstances in which they apply, and how certifications are related and used.

It is important that workforce training includes relevant standards, such as ISO 27001 and ISA/IEC 62443 (see Appendix 1). Even when not fully implemented, understanding the standards is essential to an effective cybersecurity response because they define minimum acceptable requirements for a cybersecurity program definition and operation. Expert trainers can convey the details and nuances of the standards that can form the foundations of consistent cybersecurity policies and actions, especially when in the form of non-normative guidance such as the NIST Cybersecurity Framework.

Training "boot camps" would be rapid response training operations intended to raise awareness of best practices for key manufacturing personnel, while providing a "train the trainer" resource to rapidly raise the knowledge of the maximum number of manufacturing workers, in OT and IT. Training boot camps would likely evolve and specialize over time as general understanding and awareness is achieved and training specific to industries, operations, networks, and systems becomes more critical. For example, specific training will be needed on the certification requirements of specific products and technologies provided by organizations such as the ISA Security Compliance Institute and the Institute of Electrical and Electronics Engineers (IEEE). Training offerings will also need to evolve as threats and vulnerabilities change and defensive technologies emerge.

Existing federal, state, and private resources could be mobilized and coordinated to provide these training boot camps for manufacturers. Some of the Manufacturing USA institutes, federal programs including MEP and potentially the Department of Energy's (DoE's) Industrial Assessment Centers, educational institutions, and relevant trade association, professional societies, and industry organizations are resources that could be leveraged to provide broad access to training.

MEETING CHALLENGES IN MANUFACTURING CYBERSECURITY

The July 2017 "Presidential Executive Order on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States" demonstrates the commitment by the current Administration to the strength and security of U.S. manufacturing. Multiple federal agencies already have strong programs in cybersecurity and important stakes in the cybersecurity of U.S. manufacturing (see Appendix 1). For example, the Department of Defense (DoD) programs to support and strengthen the defense industrial base have an obvious interest in manufacturing supply chain cybersecurity. With its mission to ensure robust, secure, and resilient industrial capabilities, the DoD's Office of Manufacturing and Industrial Base Policy is well positioned to address cybersecurity issues in manufacturing. The DoE maintains programs to support strong cybersecurity in energy production and distribution, especially the national electric power grid. The Department of Homeland Security (DHS) has identified four critical manufacturing sectors and has worked with industry to improve security and resilience. NIST has led the work on the Cybersecurity and Cyber Physical System Frameworks, as well as the National Cybersecurity Center of Excellence and the National Initiative for Cybersecurity Education. The National Science Foundation (NSF) funds multiple academic research efforts on cybersecurity. Other federal departments and agencies also play a role in strengthening national cybersecurity. Tying these many federal efforts together with various state and local initiatives and coordinating them with the full spectrum of private commercial, consortium, foundation, and academic initiatives would result in more effective programs and greater attention to cybersecurity in companies of all sizes.

Given the broad and pervasive scope of the issues involved, and the diversity of organizations that already play a role, a public-private partnership focused on manufacturing cybersecurity should be created to provide necessary vision and coordination and to ensure the financial resources to implement the needed testing and training infrastructure. Within the context of the Presidential Executive Order, the federal government should take the lead in forming the public-private partnership while ensuring it includes contributions from state and local governments, academia, and a broad representation from the manufacturing base. Similarly, a private organization should be chosen to manage interactions with the private sector and to ensure broad-based private sector input.

RECOMMENDATION 1: CREATE A PUBLIC-PRIVATE PARTNERSHIP FOCUSED ON MANUFACTURING SUPPLY CHAIN CYBERSECURITY.

Because of the unique characteristics of manufacturing operations and the potential extension of cyber threats through networked supply chains and digitized equipment in factories, manufacturing supply chain cybersecurity cannot be adequately addressed as the aggregated outcome of independent, uncoordinated, and localized efforts. The challenges will not be met through centralized control but through effective coordination of a decentralized national effort that can ensure the necessary local efforts have sufficient, consistent resources and expertise. The risks, challenges, and repercussions affect both the private and public sectors. Cybersecurity requirements in defense production pose particular challenges in areas such as ensuring part integrity and validation, tracking production as components move through the supply chain, and maintaining trustworthy design and production data for many years, sometimes decades. Therefore, an effective mechanism is needed for many stakeholders to work in partnership. A public-private partnership focused on manufacturing supply chain cybersecurity would provide such a mechanism. Specific tasks for such a partnership include:

- **a.** Develop a national strategy for strengthening manufacturing cybersecurity that would identify and coordinate existing public and private efforts as well as additional resources sufficient to address the diverse testing, training, and R&D needed to meet the challenges in manufacturing cybersecurity,
- **b.** Accelerate the application of existing cybersecurity technologies and practices to manufacturing to immediately lower the risks of cyberattacks,
- **c.** Coordinate facilities and mechanisms to address R&D challenges (see Chapter 3),
- **d.** Support necessary industry-wide collaboration through mechanisms such as sector-specific Information Sharing and Analysis Centers (ISACs)/Information Sharing and Analysis Organizations (ISAOs) (see Chapter 4),
- **e.** Coordinate cyber ranges and test beds to
    - i. ensure comprehensive testing for vulnerabilities and effective patching in components, equipment, software, and other aspects of networked CPS of systems,
    - ii. act as sandboxes to test new ideas safely and securely,
    - iii. provide “cyber autopsy” capabilities, and
    - iv. promote the creation of standard models for OT systems.
- **f.** Coordinate cyber ranges and test beds that will test for vulnerabilities in components, equipment, and the other myriad aspects of networked CPS of systems; act as a sandbox for new ideas; and provide “cyber autopsy” capabilities. Test beds can also promote the creation of standard models for OT systems, and
- **g.** Coordinate the development of curricula and creation of boot camps for effective training of the general manufacturing workforce in cybersecurity best practices, as well as OT and IT technical professionals in evolving threats, emerging technological solutions, effective OT/IT interface, and CPS of systems engineering.

CHAPTER 3

ESTABLISH A FEDERAL RESEARCH INITIATIVE ON MANUFACTURING CYBERSECURITY

R&D CHALLENGES AND OPPORTUNITIES

Although all manufacturers should immediately implement existing technologies and practices to mitigate cyber threats, research is needed to develop new tools and techniques. Because of the diverse and eclectic nature of digitized manufacturing technology and the integration of individual company networks throughout supply chains, this research requires funding and organization at a level higher than an individual plant or company. It must involve government, at both the state and national levels, industry, and academic institutions. The tools and techniques needed, all in the context of systems of cyberspaces, include:

1. Robust part validation technology,
2. Automated risk assessment and detection tools,
3. Tools to audit the extent and nature of attacks,
4. Sharing, prioritizing, and analyzing intelligence on emerging threats and vulnerabilities,
5. Decoys for intelligence gathering, and
6. Reference architectures with cross-cutting applicability.

ROBUST PART VALIDATION TECHNOLOGY

Because manufacturing systems typically consist of multiple, independently sourced components working together, **robust part and material validation is necessary to ensure the security of both the manufacturing systems and the products produced.** This challenge is important and unique to manufacturers because of the longevity of legacy systems and the diversity of machines and processes used.

To answer this challenge, research is needed on methodologies to provide part validation and risk assessment scoped for legacy equipment that includes:

- Techniques to identify existing attack vectors,
- Methods to anticipate future security vulnerabilities because what is not a vulnerability today could be one tomorrow (e.g., remote keys),
- Inventory systems to maintain validated part data on manufacturing parameters (where, when, and how the part was made) and lifecycle use,
- Methods to establish trust between machines of diverse ages from multiple vendors with a wide array of features and controllers, and
- Defensive capabilities based on determining how an adversary could successfully attack cyber or physical targets.

Attack graphs are one example of an existing technique used to depict system vulnerabilities and to help devise responsive security measures. Based on Red Team attack findings, these graphs are typically built manually, which limits the size of the system that can be analyzed. Development of automated attack graph generators would facilitate analysis of the large, diverse systems typically found in manufacturing.

AUTOMATED RISK ASSESSMENT AND DETECTION TOOLS

The NIST Cybersecurity Framework explains that cybersecurity risks cannot be effectively controlled until a mechanism is established to safely assess risk and detect threats using automation. Unfortunately, most current standards take the form of manual checklists. For instance, the historical method of conducting assessments involves the art of penetration testing. However, penetration testing does not scale, depends on human labor, and does not provide continuous assessment. The need for continuous assessment is particularly noteworthy because victims often have no clue when they have been attacked, in part because they have no way to detect the attack in real time. As cyber physical systems of systems grow increasingly large and interconnected, detection systems must respond more quickly and robustly than a team of humans can. **R&D is needed to create technology that can replace penetration testing with continuous, automated assessment that can be safely used in the OT environment.**

To automate risk assessment and detection, manufacturers need:

- monitoring capabilities that can verify that parts are being assembled normally,
- the ability to utilize data captured from the shop floor,
- the capability to analyze user and employee behavior,
- the capacity to monitor communication patterns for divergence, and
- technical solutions that can secure digital signatures (e.g., ledger technologies such as blockchain).

Development of common risk assessment tools is also critical. Every manufacturer, no matter how large or small, faces risk that must be managed.

It is inefficient and costly for every company to reinvent its own protection or mitigation for every new kind of threat that develops. Therefore, the research community must develop common risk assessment tools that can be tailored to unique risk models.

TOOLS TO AUDIT THE EXTENT AND NATURE OF ATTACKS

In addition to development of tools to prevent and deter cyberattacks, further research is needed to advance tools to audit the extent of successful attacks. To be confident that an attack has been fully audited, the ability to check some kind of digital signature is required because the attacker could try to cover his/her tracks. One potential solution is to use automated ledger technology, such as blockchain, to prevent the modification of digital signatures in the data. In theory, blockchain data are secure by design and could be suitable for maintaining full lifecycle data on both parts and processes.

The ability to create blockchains, or similarly secure data, in operational real time must be realized before the technology can be applied to manufacturing processes. Many research and implementation efforts are currently under way to apply blockchain technology to industries other than finance. For instance, Kouvola Innovation in Finland is testing the use of blockchains in supply chain management. A Nevada startup, Filament, is leveraging blockchain to build distributed communication networks of sensors. IBM, Intel, Philips, and other corporations are also extending the use of blockchain to areas relevant to manufacturing.[34]

SHARING, PRIORITIZING, AND ANALYZING INTELLIGENCE

For these common risk assessment and auditing tools to be truly effective manufacturers need mechanisms to share data with each other in a usable but secure fashion. ISACs/ISAOs or similar organizations (Recommendation 3) could effectively gather the collective data. Tools are needed to analyze the data, in as close to real time as possible and therefore in as automated a way as possible, to provide actionable intelligence to the manufacturing community. Patterns, trends, and impacts identified in the data would help ameliorate damage from existing attacks, while also informing the vendor and security communities of vulnerabilities, patch requirements, and ways to strengthen future system designs.

DECOYS FOR INTELLIGENCE GATHERING

Compiling the details of attacks on manufacturers and other industries is obviously necessary to create a robust data repository, but gaps are inevitable due to lax reporting or lack of knowledge that an attack has happened. Red teams and white hat hacking can help to fill some of these gaps. Another way to gather more intelligence is to use a well-structured program of decoys. The intelligence gathered from decoys, combined with the data on threats and risks collected from live breaches and discovered by white hat hackers, would allow manufacturers to identify and analyze trends to proactively improve the cybersecurity of their systems. Obviously, securing the nature of the decoys would be a paramount concern.

[34] Moody's Investor Services, "Credit Strategy—Blockchain Technology: Robust, Cost-Effective Applications Key to Unlocking Blockchain's Potential Credit Benefits," July 2016, referenced at http://www.businessinsider.com/moodys-releases-definitive-list-of-every-blockchain-project-out-there-2016-7/#-8.

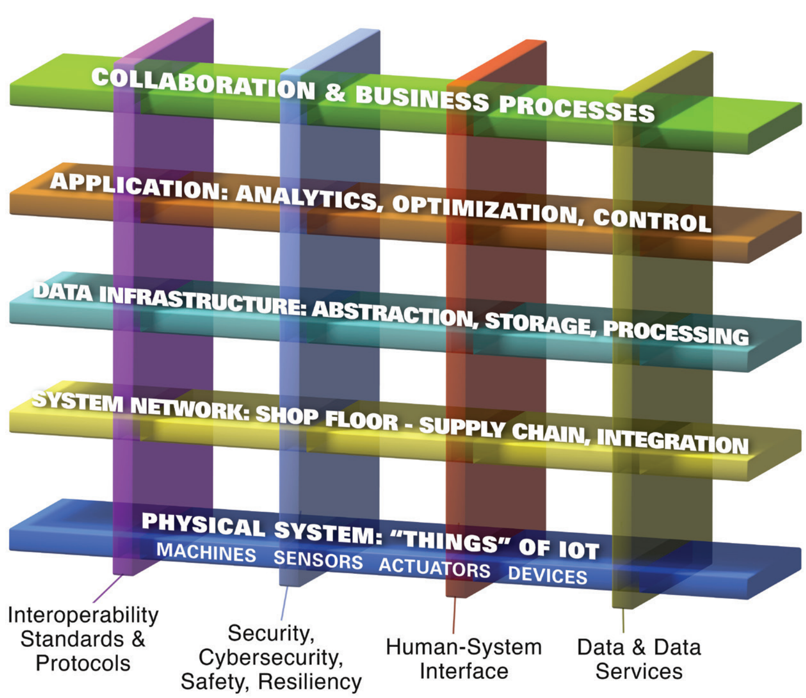
DEVELOPMENT OF REFERENCE ARCHITECTURES WITH CROSSCUTTING APPLICABILITY

In the modern age, an increasing number of industrial sensor-to-actuation, including human-in-loop, control systems are managed through computers and networked data communications. Cyber physical systems security reference architectures define the IT and OT functions, standards, and integration requirements that can be consistently addressed with a full range of manufacturing device touchpoints, a diversity of manufacturing operations and enterprises, and different vendor control, modeling, and automation platforms. The NIST CPS Framework provides guidance on the attributes of a reference architecture for manufacturing. It explains that the architecture should reflect key functional layers that are sufficiently decoupled so that each layer can be modified and replaced without unwittingly affecting the other layers. Layers typically include the physical components, networked systems, data management, applications, and collaboration and business processes. Figure 4 illustrates an example of a generalized, manufacturing-oriented reference architecture.[35]

Components that contain sensors and/or actuators should have an appropriate level of awareness of physical location and time. Characteristics of OT and IT components should be well defined using standardized component/service definitions, descriptions, and component catalogs. Support for legacy component integration and migration should include the physical artifacts, software, protocols, semantics, and other critical attributes. Data exchange is a prominent aspect and the

FIGURE 4. GENERALIZED, MANUFACTURING-ORIENTED REFERENCE ARCHITECTURE.

SOURCE: SUDARSAN RACHURI, PRESENTATION AT CLEAN ENERGY SMART MANUFACTURING INNOVATION INSTITUTE.



[35] https://www.cesmii.org/s/CESMII-Kickoff-Sudarsan-Rachuri-DOE.pdf.

nature of the data and their reliability, type, identity, and discovery are all key attributes. Data are typically "fused" or combined with other data for anonymization or enrichment, or for summarization for the benefit of users. Access is often constrained by "rights" or "privileges." To support domain flexibility, component definitions need to be flexible and open ended.

The architecture should support flexibility in virtual system creation and adaptation and a large range of application sizes, complexities, and workloads—that is, the same components that are used in a simple application should also be usable in very large, complex, distributed systems. The architecture should allow for composition from independent, decoupled components for flexibility, robustness, and resilience to changing situations. Ideally the components can be assembled and scaled quickly, even during runtime. Interfaces to these components should be based on well-defined, interpretable, and unambiguous standards. A key to supporting diversity of application and scalability is to allow internal component flexibility while providing external interoperability through standardized interfaces.

Reference architectures must be broad enough with recommended principles and layouts to work for many companies in many different sectors and must include the engineering specifications for a full range of equipment and operations. **Cyberattacks often happen between the zones of control—in the seams, so to speak. A poorly integrated system will be more vulnerable to attacks.**

Security is a necessary feature to ensure that the integrity of the information used, processed, stored, and transferred is preserved and kept confidential where needed. The nature of CPS not only increases the consequences of a breach but also introduces additional types of vulnerabilities. For example, timing in a CPS has vulnerabilities different from traditional data vulnerabilities considered in cybersecurity. Security must be built by design to ensure sufficient flexibility to support a diverse set of applications. This security should include component security and access control, as well as timing, data, and communications security. Security should also be considered in combination with other prioritized and potentially conflicting concerns, such as privacy, safety, reliability, and resilience, in a comprehensive risk management framework.

New reference architectures for these systems would improve manufacturers' awareness of the state of their cybersecurity. Additionally, provision of reference architectures for control systems and organizational/process models that are included in the design of these cyber systems will enable establishment of best practices that will increase their security. Reference architectures address the fact that many manufacturers do not know what best practices currently look like.

The reference architecture technically must be broad enough in recommended principles, structures, and layouts to work for many companies in many different sectors and provide engineering specifications for a full range of hardware and software systems. A poorly integrated CPS will be more vulnerable to attack. The principles provided in section 2 of the NIST CPS and Version 1.8 of the Industrial Internet Consortium's Industrial Internet Reference Architecture[36] provide excellent starting points for the development of the needed architectures.

CRITICAL FUNDAMENTAL R&D OBJECTIVES

Today's approach to securing systems and communications is largely monolithic and managed centrally. The advent of the Internet of Things/Internet of Everything (IoT/IoE),

[36] http://www.iiconsortium.org/IIRA.htm.

interconnected systems, and interconnected companies in smart and digital supply chains demands a decentralized approach to security in which the user/owner controls the various assets (i.e., devices and data). Dynamic business relationships that encompass cyber and physical assets will result in interconnected communication, cyberspace, data and cloud systems; multi-company partnerships and third-party responsibilities must also be considered. End-to-end management of time and actuation assumes new characteristics and introduces new kinds of vulnerabilities. **Reference architectures must design in security. Conceptual research is needed to consider the next-generation network, communications, and security architecture and management structure to avoid bolting another security solution onto today's infrastructure.** This is the type of research that the National Science Foundation (NSF) is adept at defining and funding.

A number of critical R&D activities should commence now and be supported to evolve with changing future conditions:

1. Apply systems engineering methodologies to building cyber supply chain reference architectures that design in security and resilience, treating linked cyberspaces as a systems assembly design/interface risk problem and emphasizing manufacturing security system and practice reusability. Systems engineering methods can be used to develop the systems of CPS reference architectures that account for the intra- and inter-level interfaces of cyberspace security with cross-cutting applicability.[37] As an example, the Jet Propulsion Laboratory (JPL) has evolved a design methodology known as Integrated Model Centric Engineering[38] (IMCE, and the related Model-Based System Engineering [MBSE][39]). JPL has adopted MBSE/IMCE[40] and has refined its predictive modeling and model synthesis capability under the Defense Advanced Research Program Agency's (DARPA's) F6 program.[41] This approach enables experimentation, testing, verification, and validation of various combinations of systems technologies against current processes and benchmarks in a virtual environment, and the selection of those technologies to optimize objectives before committing deployment costs. These methods can be used to create a baseline for existing technology, quantify areas of vulnerability, and identify critical priorities for improvement.

2. Create reference architectures for manufacturing IT/OT systems so that product selections can be flexible. Manufacturers will have greater trust in a reference architecture that is formed by a broad coalition of researchers with the backing of government agencies, rather than one that is distributed by a single software company. Influential cyber ranges would aid in the creation of such a reference architecture. Development of reference architectures will require a concerted, systematic, and interdisciplinary (OT/IT) engineering approach.

[37] NIST Special Publication 800-160, *Systems Security Engineering,* and ISO 15288 provide guidance for engineering trustworthy, secure systems. See R. Ross, M. McEvilley, and J. Oren, Systems Security Engineering, Nov. 2016, at https://doi.org/10.6028/NIST.SP.800-160.

[38] T. Bayer, et al., "An Operations Concept for Integrated Model-Centric Engineering at JPL," Paper #1120 IEEE Aerospace Conference, March 6-13, 2010. DOI:10.1109/AERO.2010. 5446799.

[39] J. Long, "Model-Based Systems Engineering for Project Success: The Complete Process." INCOSE International. Symposium, 20: 1502–1644, 2010. DOI: 10.1002/j.2334-5837.2010.tb01154.x.

[40] T. Bayer et al., "An Operations Concept for Integrated Model-Centric Engineering at JPL," Paper #1120 IEEE Aerospace Conference, March 6-13, 2010. DOI:10.1109/AERO.2010. 5446799.

[41] S. Cornford, et al., "Evaluating a Fractionated Spacecraft System: A Business Case Tool for DARPA's F6 Program," IEEE Aerospace Conference, March 3-10, 2012. DOI:10.1109/AERO. 2012.6187435.

3. Develop systems of systems architecture that integrate design and analysis with cloud services. Designing the security of multiple things is as important as automated checking and validation. The cloud is just someone else's computer. Cloud connections are more numerous and pervasive than many managers realize, which implies the need for policies to delineate appropriate connection procedures.

4. Define and develop a supply chain cybersecurity framework that includes robust part validation technologies, methods to audit attacks and responses, a common language across multiple functional departments, and application of appropriate standards such as ISA/IEC 62443 and ISO 27001.

5. Develop a framework of hardware and software "trust anchors" for on-demand party-to-party and party-to-multi-party compartmentalized data management with manufacturing hardware and software systems. Most current strategies focus on ensuring local processing of data, which is likely a short-term solution.

CRITICAL NEAR-TERM R&D OBJECTIVES

R&D activities that would contribute to critical near-term objectives include:

1. Take advantage of cyber supply chain security opportunities from systems of systems engineering approaches. **If Secure A + Secure B is NOT secure, then what must be done to A and B together to make A + B secure or to mitigate impacts?** How can systems security be verified and validated rapidly when cyberspaces are brought together for business purposes? Applying a systems methodology would illuminate the existing taxonomy of relevant standards and compare these standards with an ideal state model to identify gaps and ways to address them. Using this ideal state model, "levels" of cybersecurity for manufacturers could be defined and described.

2. Develop automated tools for assessing risk, detecting attacks, and determining the extent of attack. Many such tools currently exist, but they are not tuned for manufacturing use or the operational requirements of a production setting. Research is needed to determine how to use these IT tools in an operational setting. In particular, development of analytics-based detection tools for both IT and OT and use of digital twins would be beneficial to manufacturing applications.

3. Develop automated, robust part validation technology to assure that parts meet design specifications and to track part providence throughout the supply chain from initial production through final assembly and customer delivery. Automated ledger technology such as blockchain shows promise for application in manufacturing to create trusted environments.

Achieving these critical near- and long-term technologies, tools, and architectures requires a research program focused on the cybersecurity needs of existing and evolving manufacturing systems. The federal government should:

RECOMMENDATION 2: ESTABLISH A FEDERAL RESEARCH INITIATIVE TO ADDRESS BOTH NEAR- AND LONG-TERM CYBERSECURITY CHALLENGES AND OPPORTUNITIES IN MANUFACTURING.

Fundamental research should address systems-of-systems engineering methodologies for cyber physical systems with designed-in cybersecurity and resilience, treating linked cyber spaces as systems design/interface risk problems. Critical development activities that should commence now and require support to evolve include:

a. Create systems and security reference architectures for manufacturing that define the OT and IT functions, standards, and integration requirements. The reference architectures should be applicable across a diverse range of manufacturing devices, operations, and enterprises, and different vendor control, modeling, and automation platforms.

b. Establish software and hardware trust anchor frameworks for securely connecting and managing many devices, systems, and data in manufacturing systems without central management.

c. Develop systems-of-systems architecture design and analysis that integrate with cloud services.

R&D activities that would contribute to critical near-term objectives include:

a. Automated vulnerability assessment and detection tools. Many tools currently exist but are not tuned for manufacturing or the operational requirements of a production setting.

b. Analytics-based detection—networks or machines—and use of digital twins.

c. Tools to audit the extent of attacks.

d. Automated, robust part validation technology, including automated distributed ledger technologies such as blockchain, for trusted parts and data validation.

CHAPTER 4

ESTABLISH MECHANISMS FOR INDUSTRY COLLABORATION

STRONG CYBERSECURITY REQUIRES COLLABORATION

Leaders in private industry and government are becoming increasingly aware that security is a major issue for manufacturers as both production facilities and multiple product segments become connected. This "connectedness" will cause a massive increase in the number of networked devices. **Qualification of the parts, materials, models, sensors, controllers, and processes, while protecting the IP they embody, will require stringent multi-industry, multinational cooperation.**

Trade associations, professional societies, and other groups could provide the mechanism for the needed collaboration, but models used widely in other industries are instructive. ISACs/ISAOs provide a mechanism for cooperation among companies in similar industries to facilitate fault-free, anonymous sharing of incidents, threats, vulnerabilities, best practices, and solutions (see Box 1).[42] Some existing ISACs/ISAOs include manufacturers as members, but none are focused on manufacturing.

Manufacturing ISACs/ISAOs could:

1. Develop a data repository of anonymous submissions of cyberattacks. A data repository with anonymized data from many companies that allows manufacturers to identify and analyze trends would be a boon to both the manufacturing and the cybersecurity research communities.

[42] In February 2015, President Obama issued Executive Order 13691 promoting private-sector cybersecurity information sharing that directed the Department of Homeland Security (DHS) to encourage the development of ISAOs and to create an ISAO standards organization. Details can be found at https://www.dhs.gov/isao.

BOX 1. ISACs AND ISAOs

INFORMATION SHARING AND ANALYSIS CENTERS

Information Sharing and Analysis Centers (ISACs) are sector-specific membership organizations that facilitate sharing information on cyber and physical threats. Typically member-driven non-profit organizations 22 ISACs currently operate, focused on critical infrastructure sectors such as financial services, electricity, healthcare, and oil and natural gas. At least four ISACs—Automotive, Aviation, Defense Industrial Base, and Supply Chain—have manufacturers as members. The Automotive ISAC limits membership to light and heavy-duty vehicle OEMs and suppliers and commercial vehicle companies. The Aviation ISAC includes airlines, airports, satellite, engine, and equipment segments of the industry. Membership in the Defense Industrial Base ISAC is open to companies with responsibility for protection of the defense industrial base infrastructure.

INFORMATION SHARING AND ANALYSIS ORGANIZATIONS

Information Sharing and Analysis Organizations (ISAOs) are organized more broadly than ISACs, often based on geographic regions, such as Northeast Ohio, Maryland, and Arizona, as well as industries such as legal services, credit unions, and retail. Among the 23 ISAOs, some include manufacturing members: the Medical Device ISAO and the IoT ISAO are examples. In 2015, the DHS funded the ISAO Standards Organization at the University of Texas to identify a set of voluntary standards for the creation and functioning of ISAOs.

2. Facilitate the implementation of decoys for intelligence gathering. Although compiling the details of attacks on manufacturers and others is obviously necessary to create a robust data repository, relying only on the data from noticed and/or reported attacks forces responders to wait until a threat occurs in the wild. Red teams and white hat hackers can help fill some of these gaps. Another way to gather more intelligence is to use decoys. The intelligence gathered from decoys, combined with the data on threats and risks collected from live breaches and discovered by white hat hackers, would allow manufacturers to identify and analyze trends proactively to improve the cybersecurity of their systems.

3. Facilitate the prioritization and sharing of intelligence. Intelligence sharing might best be accomplished through a public-private partnership that could take advantage of the intelligence-gathering capabilities of federal agencies such as DHS and DoD, combined with the industry coordination and reporting provided by the industry-specific ISACs/ISAOs.

ISACs/ISAOs should become a trusted, integral part of the national manufacturing ecosystem, but they can only be effective if manufacturers join/form relevant ISACs/ISAOs and actively participate in them by sharing data and acting on the resulting intelligence. In turn, active participation can only be expected if the current complacency among manufacturers is overcome.

COMPLACENCY: BARRIER TO COLLABORATION

Perhaps the single greatest obstacle to strengthening cybersecurity in manufacturing is complacency among manufacturers. **Because there has not been a reported major incident in U.S. manufacturing, there is not sufficient financial or regulatory incentive to move beyond cursory action.** Cyberattacks in other industries, regardless of their similarity to manufacturing, such as the recent well-known attacks on Sony, Target, and Yahoo, have not been a sufficient motivator to manufacturers to invest in cybersecurity. SMMs—typically defined as manufacturers with fewer than 500 employees—comprise greater than 90 percent of the U.S. manufacturing base but do not see security as a threat to their operations, do not perceive a competitive advantage to investing in security, and often cannot afford the cost of IT professionals skilled in cybersecurity.

Lack of incentive to act is compounded by significant lack of understanding (or confusion) on what actions to take. Few manufacturers have staff with the skills needed to address cybersecurity challenges. The multifaceted impacts of a cyberattack not only on production but also on occupational health and safety, insurance, liability, and financial compliance are only just being recognized.

The pervasive, serious, and rapidly evolving nature of cyber threats to manufacturers of all sizes in all industries requires flexible, cost-effective solutions best driven by market incentives rather than by regulatory requirements. Cybersecurity needs to become an ingrained part of every manufacturer's culture, embedded in management decisions, workforce training, and investment calculations.

An obvious analogy is the emergence of a quality culture in the 1980s, initially driven by Japanese competition but eventually becoming pervasive throughout U.S. manufacturing. Having a formal system in place to assure high-quality production, often based on ISO 9001 and related standards, is frequently a condition for winning business with OEMs. Similar broad adoption of cybersecurity standards, such as ISA/IEC 62443 and ISO 27001 (see Appendix 1), driven by requirements from large customers and filtering through supply chains, could provide a competitive advantage and the market demand needed for manufacturers to invest in cybersecurity.[43]

Another potential market driver of stronger cybersecurity practices is creating a price mechanism that would value strong cybersecurity. Cybersecurity insurance is one such mechanism. In a recent survey of global risk management, Aon found that cybercrime is the top concern of businesses in North America among all respondents but it was not one of the top three concerns among manufacturers. The smaller the company, the less likely cybersecurity was named as a high risk. Of the companies surveyed, **manufacturing companies were among the least likely to buy cyber insurance, and few manufacturers have tried to quantify the potential costs of a cyberattack.**[44] Without financial impact metrics, the needed investments to mitigate the risks of cyberattacks are difficult to justify.

Here, too, collaboration is essential to share information on the frequency and nature of cyberattacks, their impacts on the affected businesses, and steps businesses take to ameliorate the impacts and to recover quickly from the attacks. If market incentives were created that encourage manufacturers to purchase cybersecurity insurance, then manufacturers would also have incentive to share information as a way to ensure premiums are both fair and minimized.

[43] The system used by Six Sigma practitioners to designate levels of expertise and experience by "belt" color (i.e., green, black, master black) might also be applied to cybersecurity professionals.

[44] Aon, 2017 *Global Risk Management Survey*.

Creating the needed market incentives and sufficient participation in collaborative organizations can only be accomplished by senior corporate leadership. A working group of Chief Executive Officers (CEOs) from a representative cross-section of manufacturing industries, combined with senior government officials and academics, could raise and maintain awareness on cybersecurity in manufacturing. Specific action items for this working group include:

1. **Create market incentives for strong cybersecurity similar to the national "quality assurance" program that emerged in U.S. manufacturing in the 1980s.**[45] Awareness, conviction, adoption, and execution of cybersecurity measures must become a competitive advantage within organizations throughout the manufacturing sector. Ideally, solutions will be market rather than regulation driven to ensure long-term flexibility and incentives for continuous improvement. Industry groups should work with government to facilitate awareness and education and to support efforts to define the implications of cybersecurity incidents. Industry should lead the discussions to advance common understanding of how cybersecurity incidents will be handled, including information sharing, mitigation, and solutions.
2. Create a cybersecurity standards registration program, similar to ISO 9001 and other related quality systems, that defines effective cybersecurity policies and practices and confirms the organizations' commitment to continuous improvement. The ISA/IEC 62443 and ISO 27001 standards for cybersecurity provide readily available mechanisms to gage manufacturers' cybersecurity practices. Like quality systems, independent auditors would confirm that effective cybersecurity efforts are in place, and markets would favor manufacturers with the cybersecurity registration.
3. Form a national cybersecurity certification laboratory to eliminate the need for each company to test every product/process. Underwriters Laboratory could serve as a model.[46] Certification would require definition of a base level of security for software and hardware for products and processes.
4. Encourage all manufacturers, regardless of size or industry, to participate in industry-specific ISACs and to implement the cybersecurity practices identified in the Repeatable and Adaptive Implementation Tiers in the NIST Cybersecurity Framework. To help smaller firms, the working group should encourage them to work with their local MEP center to implement the Cybersecurity Framework practices and to become compliant with the Defense Federal Acquisition Regulation Supplement (DFARS) on cybersecurity (see Appendix 1).
5. Working with appropriate involvement from government and academia, converge on an overall taxonomy, guidelines, and standards for IT/OT interfaces, authentication, protection from different caliber of attacks, and procedures for reporting attacks.
6. Learn from and apply approaches already in use in the financial and energy sectors.

Creating the needed market incentives and mechanisms for essential multi-company collaboration can be accomplished with the following actions:

[45] Kenneth Krieg, presentation to MForesight Cybersecurity Workshop, March 14, 2017.
[46] http://industries.ul.com/cybersecurity.

RECOMMENDATION 3: ESTABLISH MANUFACTURING INDUSTRY-SPECIFIC ISACS, ISAOS, OR SIMILAR ORGANIZATIONS.

ISACs/ISAOs, or similar industry-led organizations, can facilitate fault-free, anonymous sharing of incidents, threats, vulnerabilities, best practices, and solutions. Proactive collaborative activities that manufacturing-specific ISACs/ISAOs could initiate include:

a. Develop a data repository of anonymous submissions of cyberattacks, and disseminate anonymized reports to manufacturers on a regular schedule,

b. Coordinate use of decoys for intelligence gathering and sharing,

c. Create industry test beds, cyber ranges, and demonstration facilities to safely prototype and test OT and IT security technologies, identify system-level vulnerabilities, and provide a "cyber autopsy" capability, and

d. Identify and disseminate best practices and provide training platforms/curricula.

RECOMMENDATION 4: ESTABLISH AN EXECUTIVE-LEVEL WORKING GROUP.

An executive-level working group is needed to provide a strong industry voice to advocate for and motivate industry action to strengthen cybersecurity. Using quality system certifications as a model, the working group should drive market-based incentives for stronger cybersecurity in manufacturing. The goal should be for most manufacturers to implement the practices identified in the Repeatable and Adaptive Implementation Tiers in the NIST Cybersecurity Framework, and to meet the requirements detailed in relevant standards such as ISA/IEC 62443 and ISO 27001. The working group should also:

a. Promote participation by all manufacturers in their industry's ISAC/ISAO,

b. Facilitate the emergence of financial risk management procedures that can apply to cybersecurity practices, and

c. Communicate with executives in other at-risk economic sectors such as finance and energy to ensure that solutions developed for those industries are applied in manufacturing.

CHAPTER 5

CREATE A FRAMEWORK FOR SUPPLY CHAIN CYBERSECURITY

CYBER PHYSICAL SYSTEM SECURITY IN MANUFACTURING

Manufacturing is the orchestration of multiple operations that move and change materials and assemble parts into market-driven end products that meet customer needs. In addition to factories, manufacturing enterprises include research facilities, distribution centers, business management operations, and a host of vendors and suppliers that form extensive value chains. Competitive imperatives require that products be produced consistently, predictably, and with zero safety incidents, with well-defined precision, and at as low a cost and as low an impact on the environment as possible. Each manufacturing operation consists of people, material handling and processing equipment, sensors, control systems, models, and the data that emanate from them.

Manufacturing combines complex OT with multiple levels of data, control systems, and networks, that require attention to OT and IT together throughout the enterprise. This combination of OT and IT systems is referred to as cyber physical systems.[47] Manufacturing cyber supply chains are dominated by systems of CPS that bridge multiple purposes, time, and data domains.

Manufacturing still functions with a large base of old but still serviceable equipment and

[47] As defined in the NIST CPS Framework, CPS are smart systems that include engineered interacting networks of physical and computational components.

operations; therefore, cybersecurity risks are not confined to advanced, automated factories. Risks are aggravated by old, digital controls but can be mitigated by proprietary, closed system deployments. As manufacturers invest in networking old systems and new advanced sensors, modeling, control, robotics, Asset Performance Management (APM) systems, and enterprise resource planning (ERP) systems across supply chains, security risks increase because the number of CPS increases and networks become more complex.

The sheer growth of digital devices and systems deployed throughout manufacturing has already created a large deficit in the number of workers with the necessary cybersecurity systems expertise. **The potential number of "weakest-link" cyberattack vulnerabilities is a function of constantly evolving technology, gaps in organization and workforce skills, growing numbers of CPS interfaces, and increasingly numerous and sophisticated cyberattacks.**

DIGITIZED, NETWORKED MANUFACTURING: OPPORTUNITY AND RISK

Key characteristics of manufacturing make industry inherently vulnerable to cyberattack. Yet trends in automation, computerization, and networked and tightly integrated supply chains, and the emergence of the IoT introduce new vulnerabilities that will be increasingly difficult to manage unless appropriate, sufficient investments are made soon. These trends are driven by a combination of market demand and the availability of new technologies that provide not only new functionality but also new sources of risk.

Customer demand for product diversity and customization is forcing manufacturers to adapt quickly with flexible, dynamic operations. New materials, sophisticated design and modeling tools, advanced computer controls, and real-time production and market information enable manufacturers to respond rapidly to changing customer needs. Pressure to be more flexible pushes deep into supply chains,[48] affecting multiple organizations and requiring a level of communication through integrated ERP and operational systems that automate supply chain management. The cybersecurity landscape is one of increasing precision, frequent change, and dynamic production such that reference behaviors, operations, data flows, and data patterns also should be established dynamically.

The proliferation of digital devices and data applications that must be interoperable within a given company and across multiple companies in a supply chain creates substantial management challenges. **With many responsible parties, the total system-of-systems cannot be readily or centrally managed, and cannot be treated as a collection of individual, compartmentalized systems.** Achieving essential interoperability is becoming more difficult as complexity increases. Simply retrofitting existing supply chain management applications raises overall system and security complexity. A new approach is needed that begins with the simplest problems and that draws on reusable, rather than generative, data application design and engineering.

For example, every device that generates or acts on data needs a "trust anchor" that not only grants an authorized user access to necessary data at a granular level but also limits that user's access to what is necessary. Trust anchors standardize how data and ownership for each hardware and software component in a system is documented. They enable business-to-business data agreements to be managed securely at the

[48] For more details on next-generation supply chains, see the recent MForesight report, T. Mahoney and S. Helper, *Ensuring American Manufacturing Leadership Through Next-Generation Supply Chains,* Ann Arbor, MI: MForesight, 2017.

right levels of granularity. The trust anchor also records details about how access was gained. Put simply, the set of entities that can create, read, copy, and/or modify data on any given device must be controlled. In manufacturing, trust anchors need to be engineered to avoid introducing delay into the production control networks. There is a reasonable amount of risk that, without such trust anchors, these hardware and software systems will be security break-entry points, especially as more devices are interconnected through the IoT.

CYBERSECURITY AND CYBER PHYSICAL SYSTEMS FRAMEWORKS

NIST has developed a Framework for Improving Critical Infrastructure Cybersecurity, and its public working group is developing a Framework for Cyber Physical Systems.[49] The NIST Cybersecurity Framework (CSF) is a risk-based approach to managing cybersecurity consisting of three parts: Framework Core, Framework Implementation Tiers, and Framework Profiles, summarized as follows:

1. The **Framework Core** is a set of activities and desired outcomes that are common across critical infrastructure sectors. It consists of five functions: Identify, Protect, Detect, Respond, and Recover, which together provide the basis for strategic management of cybersecurity risks.

2. **Framework Implementation Tiers** describe the extent to which an organization's cybersecurity management practices are mature and pervasive. Within each Tier, an organization's cyber risk management is assessed in four areas: Risk Management Process, Integrated Risk Management Program, External Participation, and Cyber Supply Chain Risk Management. The four Tiers include:

   1. **Partial**—In this tier, risk management practices are not formalized. There is limited awareness of cyber risk at an organizational level and no processes to collaborate with external organizations. The firm does not understand supply chain risks and has no processes in place to identify or mitigate them.

   2. **Risk informed**—Risk management practices are formalized, but an organization-wide approach is not established. The organization is aware of its role in a larger ecosystem but has no formalized capability to interact or share information. The firm understands cyber supply chain risks but has no formal programs to manage the risks internally or with its suppliers.

   3. **Repeatable**—Risk management practices are formally approved, expressed as policy, and regularly updated. Consistent methods are in place to monitor risk consistently, respond effectively, and communicate across the organization. The organization understands external dependencies, enabling collaboration. Enterprise risk management policies, processes, and procedures are used to manage cyber supply chain risks; formal agreements are in place to communicate baseline requirements to suppliers and partners.

   4. **Adaptive**—The organization actively adapts to lessons learned. An integrated risk management program recognizes the relationship between business objectives and cybersecurity risk, and includes a

[49] Cyber Physical Systems Public Working Group, *Framework for Cyber Physical Systems*, Release 1.0, May 2016.

budget based on current and predicted risks. Cybersecurity risk management is part of the culture, focused on continuous improvement. Real-time or near real-time information is shared with suppliers and partners proactively; both formal and informal mechanisms are used to maintain strong relationships throughout the supply chain.

Organizations in Tier 1 (Partial) are encouraged to move up at least one Tier, but Tiers do not represent maturity levels. Each organization judges what combination of management practices is appropriate for its situation to reduce cybersecurity risk in a cost-effective manner. **For manufacturers, greater attention to supply chain risk management must necessarily be a high priority in reducing their cyber risk profile.**

3. **Framework Profiles** are the alignment of standards, guidelines, and practices in a particular implementation of the Framework Core. A "current state" Profile can identify existing activities, risks, and business drivers to assess the organization's current level of cyber risk, then use the current Profile to establish priorities and initiatives to achieve a desired "future state" Profile. The Profiles can be used, in the context of the Framework Core and Implementation Tiers, to conduct self-assessments and to provide the basis for consistent direction and communication within and between organizations.

The CSF provides general guidelines for sound cybersecurity management practices and is broadly applicable to multiple types of organizations, including manufacturers. For relatively unsophisticated companies, the CSF provides a good primer on basic cybersecurity practices and a roadmap for improving those practices applicable to any level of corporate sophistication and resources. The Framework for Cyber Physical Systems includes more technical detail addressing the complex device and equipment interactions typical in a manufacturing environment.

CYBER SUPPLY CHAIN SECURITY AND RESILIENCE

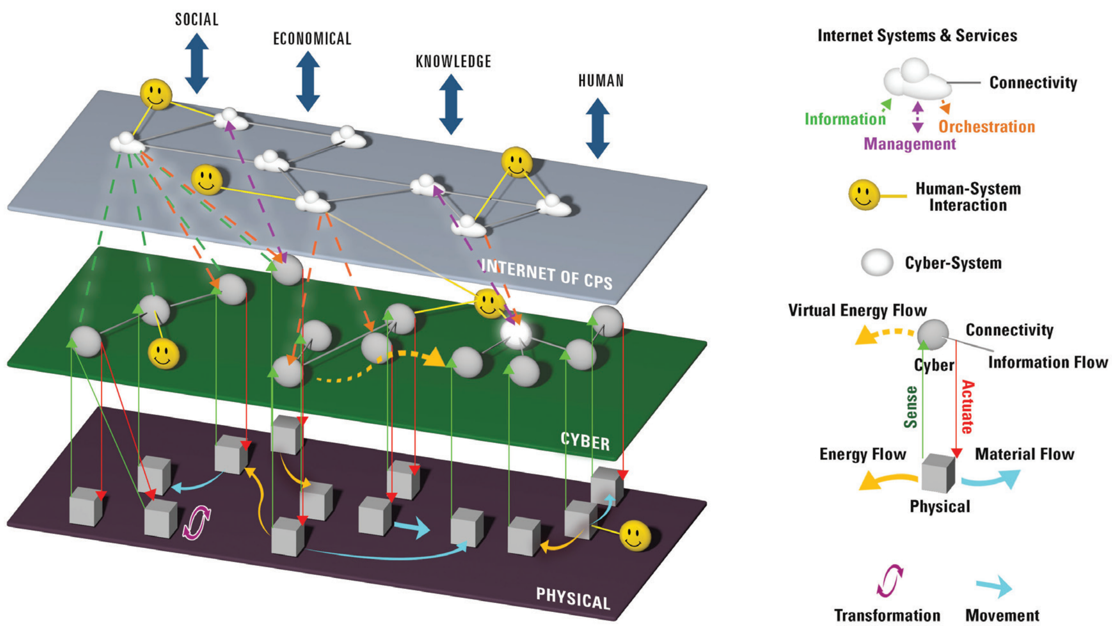
OT refers to any physical operating equipment at any level of the production process (i.e., machine, process, line operation, factory). In modern factories, OT is connected using IT networks defined by the role of the equipment in the production process. OT/IT levels include:

1. Devices (e.g., sensors, equipment, and actuators) that are associated with or connected to local factory information and data systems (often multiple),
2. Combinations of devices that form an operation within a factory and are connected to a factory operation cyberspace or linked cyberspaces,
3. Combinations of operations that form a line operation within a factory and are connected to a factory cyberspace or to linked cyberspaces,
4. Combination of line operations within a company that form cross-factory enterprise operations and are interconnected to multiple company cyberspaces, and
5. Combinations of line operations and/or company enterprise operations that form supply chain enterprises and involve inter-company, interconnected cyberspaces.

Cyber supply chain security and resilience implies that security and resilience comprise nested security practices. Each time cyberspaces are interconnected to create a new operational level, a new, higher level cyberspace is generated for which security must be addressed as a combination of cyberspaces. Expressed in terms of the NIST CPS framework, cyber supply chains are systems of CPS in which the architectural constructs of each of the cyberspace levels are applied recursively or iteratively to create a nested structure. Figure 5 illustrates the functional composition of CPS as a system-of-systems.

FIGURE 5. FUNCTIONAL COMPOSITION OF CPS AS A SYSTEM-OF-SYSTEMS.

SOURCE: CYBER PHYSICAL SYSTEMS PUBLIC WORKING GROUP



This combination of cyberspaces, increasingly essential in manufacturing, raises two critical points that complicate security, namely:

a. Secure A at any level + Unsecure B at any level results in Unsecure (A + B)

b. Secure A at any level + Secure B at any level does **NOT** equal Secure (A + B)

Cyber supply chain security and resilience require not only each organization to address internal Core and Profile Frameworks but also a highly collaborative, cross-company approach to build a security framework for the total supply chain ecosystem.[50]

Five priority areas of emphasis drive manufacturing-specific cyber supply chain security needs. These relate directly to the manufacturing-specific attributes listed above:

1. **System-level security and cyber-resilience:** Cybersecurity starts with the technical and organizational cores and processes for factory-level information and data security.
2. **Integrity of manufactured goods from design through the factory floor:** Cyber supply chain security must be defined and addressed in terms of product qualifications, chain of custody, validated manufacturing conditions and supplier data integrity, and legacy operating equipment.
3. **Securely connecting the factory to the supply chain:** Market and technology dynamics increasingly dictate that all factories build cyberspaces that can digitally connect to other cyberspaces to form an overall supply chain cyberspace, a system- of-systems. The multiple organizations forming these supply chain cyberspaces cannot be subject to weakest link security, creating an imperative for all suppliers to maintain robust cybersecurity as a condition for participation.

[50] Mahoney and Helper, p. 39.

4. **Cyber intelligence (gathering, assessing, and sharing):** As defined in the NIST CSF, an organization at the Repeatable or Adaptive Framework Tiers understands external dependencies, enacts cyber supply chain risk management, uses risk informed processes, manages risk, actively shares with partners, and can quickly account for emerging cybersecurity supply chain risks.

5. **Machine-to-machine security, especially legacy systems:** Cybersecurity supply chain security must address a very large diversity of manufactured products, machines, operations and configurations, and an extensive and heterogeneous base of proprietary systems.

Progress in these areas requires additional attention on manufacturing cyber supply chain security.

RECOMMENDATION 5: DEVELOP A FRAMEWORK FOR MANUFACTURING SUPPLY CHAIN CYBERSECURITY.

Similar to existing frameworks on cybersecurity and cyber physical security, a comprehensive framework should be developed specifically for manufacturing supply chain cybersecurity. It should reference:

a. robust part validation technologies,

b. methods to audit attacks and responses,

c. a common language across multiple functional departments and organizations, and

d. application of appropriate standards such as ISA/IEC 62443 and ISO 27001.

APPENDIX 1

INITIATIVES BY GOVERNMENT AND STANDARDS ORGANIZATIONS

In addition to the National Institute of Standards and Technology (NIST) Cybersecurity and Cyber Physical System Frameworks, several other government and nongovernment initiatives are addressing various aspects of cybersecurity in manufacturing. Though not an exhaustive list, the most relevant to manufacturing include the Department of Defense (DoD), the Department of Commerce (DoC), the Department of Homeland Security (DHS), the Department of Energy (DoE), the International Standards Organization (ISO), and the International Society of Automation (ISA).

One of the most impactful initiatives is the DoD's implementation of cybersecurity Defense Federal Acquisition Regulation Supplement (DFARS) (see Box 2). By requiring contractors and subcontractors to implement information security management controls based on NIST's 800-171 documentation, the DFARS have focused attention on cybersecurity among many industrial companies. Several consultancies are working with contractors to meet the December 31, 2017 deadline for compliance. NIST's Manufacturing Extension Partnership (MEP) program has also started an initiative to assist its client base of small and medium-sized manufacturers (SMMs) to achieve compliance. However, NIST 800-171 addresses general cybersecurity practices, not industrial control systems. A separate document, NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," addresses supervisory control and data acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and other control system configurations.

The DoD has a Cyber Crime Center (DC3), which serves as the operational focal point for the defense industrial base cybersecurity program. DC3 provides digital forensic services, technical training, solutions development, and analytics for several defense mission areas.[51] DC3 includes the Defense Industrial Base Collaborative Information Sharing Environment (DCISE), the single DoD focal point for receiving all cyber incident reporting affecting unclassified networks of defense contractors.[52]

The Defense Science Board released the report of the Cyber Supply Chain Task Force in February 2017, which addresses many of the issues of concern to manufacturing cybersecurity.[53] The Task Force examined risks to the defense supply chain, how to mitigate vulnerabilities, and how to manage acquisition to support lifecycle operations and minimize risk. The task force recommended steps to strengthen lifecycle protection policies, enterprise implementation support, and R&D programs to ensure that DoD weapons systems are designed, fielded, and sustained in a way that reduces the likelihood and consequences of cyber supply chain attacks.

At NIST, in addition to the NIST CPS and Cybersecurity Frameworks, the "Guide to Industrial Control System Security," the work of MEP in cybersecurity, and the cybersecurity test bed, the Baldrige Program supports cybersecurity. The Baldrige Cybersecurity Excellence Builder is a self-assessment tool based on the Cybersecurity Framework that is intended to help organizations improve their cybersecurity risk management efforts.[54]

NIST also houses the National Cybersecurity Center of Excellence (NCCoE), a hub for industry organizations, government agencies, and academic institutions to collaborate on cybersecurity challenges and develop practical solutions. In March 2017, the NCCoE released "Capabilities Assessment for Securing Manufacturing Industrial Control Systems," the first in a four-part series describing its project in ICS security. Each part will address one of four cybersecurity capabilities: Behavioral Anomaly Detection, ICS Application Whitelisting, Malware Detection and Mitigation, and ICS Data Integrity. For each capability, the NCCoE will map the security characteristics to the Cybersecurity Framework and implement each in lab settings at NIST. The four-part project will result in a Cybersecurity Practice Guide with detailed implementation guidelines of practical steps to improve cybersecurity.[55]

NIST also leads the National Initiative for Cybersecurity Education (NICE), a partnership between government, academia, and the private sector that focuses on cybersecurity education, training, and workforce development. NICE coordinates public and private efforts to build a strong network of cybersecurity

---

[51] http://www.dc3.mil/.

[52] http://www.dc3.mil/cyber-security.

[53] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on Cyber Supply Chains,* Washington, D.C.: February 2017.

[54] https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative.

[55] K. Stouffer and J. McCarthy, "Capabilities Assessment for Securing Manufacturing Industrial Control System," NIST Engineering Laboratory and National Cybersecurity Center of Excellence, March 2017.

BOX 2. DFARS THAT ADDRESS CYBERSECURITY.

DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT

Several DFARS addressing cybersecurity impose a number of requirements on contractors and subcontractors for managing data security and include a December 31, 2017 deadline for compliance. Table 1 highlights the key requirements in the Cybersecurity DFARS.

SUBPART	TITLE	REQUIREMENTS
204.73	Safeguarding Covered Defense Information and Cyber Incident Reporting	• Contractors and subcontractors must safeguard covered defense information that resides in or transits through contractor unclassified information system. • Incidents involving possible loss of covered data must be rapidly reported via dibnet.dod.mil.
252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting	• Contractors will implement information systems security protections on all covered Contractor unclassified information systems. • Contractors must implement security requirements in NIST 800-171 as soon as practical but not later than December 31, 2017. • For all contracts awarded prior to October 1, 2017, the contractor must notify the DoD Chief Information Officer, within 30 days of the contract award, of any security requirements specified by NIST 800-171 not implemented at the time of award. • Contractors must apply other information system security measures whenever additional security measures are required. • If Contractors intend to use cloud services for defense information, the cloud service must meet security requirements equivalent to those established for the Federal Risk and Authorization Management Program. • Incidents must be reported within 72 hours to both the prime contractor and the DoD. • Malicious software discovered and isolated by Contractors should be submitted to the DoD Cyber Crime Center. • Contractors must include these requirements in subcontracts, and require subcontractors to notify the Contractor when requesting variance from NIST 800-171 and whenever incidents occur.

education and training programs to increase the number and skills of cybersecurity professionals across all economic sectors.[56]

Another DoC initiative related to manufacturing cybersecurity is the National Telecommunications and Information Administration's program to increase the security of the Internet of Things (IoT). This initiative is a multi-stakeholder process to address security vulnerabilities in IoT devices through patching and upgrades. The goal of the program is to develop common definitions to describe security upgradability and to provide more transparency in how patches or upgrades are deployed to IoT devices and applications.[57] Several multi-stakeholder meetings have been held and are planned in 2017, and working groups formed, to address IoT security.[58]

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at DHS works across all critical infrastructure sectors to reduce risk and coordinate responses to control systems-related cybersecurity incidents.[59] Within critical infrastructure, DHS has identified four critical manufacturing sectors (Box 3), and has established a Critical Manufacturing Sector Coordinating Council. In 2015, the Council issued the Critical Manufacturing

BOX 3. CRITICAL MANUFACTURING SECTORS.

1 PRIMARY METALS MANUFACTURING

- Iron and steel mills and ferro alloy
- Alumina and aluminum production and processing
- Nonferrous metal production and processing

2 MACHINERY MANUFACTURING

- Engine and turbine manufacturing
- Power transmission equipment manufacturing
- Earth moving, mining, agricultural, and construction equipment manufacturing

3 ELECTRICAL EQUIPMENT, APPLIANCE AND COMPONENT MANUFACTURING

- Electric motor manufacturing
- Transformer manufacturing
- Generator manufacturing

4 TRANSPORTATION EQUIPMENT MANUFACTURING

- Vehicles and commercial ships manufacturing
- Aerospace products and parts manufacturing
- Locomotives, railroad and transit cars, and rail track equipment manufacturing

---

[56] https://www.nist.gov/itl/applied-cybersecurity/nice/about.

[57] A. Simpson, "Increasing the Potential of IoT Through Security and Transparency," at https://www.ntia.doc.gov/blog/2016/increasing-potential-iot-through-security-and-transparency.

[58] https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

[59] https://ics-cert.us-cert.gov/.

Sector-Specific Plan, which is designed to guide voluntary, collaborative efforts to improve security and resilience, including cybersecurity.[60]

DoE has a strong program focused on cybersecurity for critical energy infrastructure, which often uses industrial control systems (ICS) that are similar to those used by manufacturers. DoE's Office of Electricity Delivery and Energy Reliability has an extensive program on cybersecurity for energy delivery systems, including both operations and R&D programs. The operations program aims to use existing technology to increase cybersecurity in the energy sector. Initiatives include models and system analysis tools to help utilities conduct self-assessments and to prioritize investments to improve cybersecurity; the Cybersecurity Risk Information Sharing Program (CRISP) to enable quick communication among utilities on incidents, threats, and mitigation measures; and other initiatives related to utility operations to help them raise cybersecurity as easily as possible. The R&D program works through partnerships among 10 national laboratories, 30 utilities, 30 suppliers, and 25 universities to fill gaps in research that will provide stronger security with fewer resources. A roadmap was released in 2006 and updated in 2011 to identify research needed to ensure that the electric grid can survive and quickly recover from cyberattacks. More than 100 research projects have been funded since 2010, resulting in more than 35 software, firmware, and hardware tools to strengthen cybersecurity in the electricity industry.[61]

Nongovernmental organizations, particularly standards organizations, are also active in industrial cybersecurity. For several years, the ISA has worked with the American National Standards Institute (ANSI) on security standards for industrial automation and control systems. This effort created the ISA99 committee, which currently includes more than 500 members representing organizations and industry sectors worldwide. The ISA99 committee works with the International Electrotechnical Commission (IEC) to develop the ISA/IEC 62443 series of standards on industrial automation and control systems security.[62] The series addresses product development and component security requirements, system-level security technologies, policies and procedures, and conformance metrics, among other details.

Examples of published standards in the ANSI/ISA 62443 series include:

- ANSI/ISA-62443-1-1: Concepts and Models
- ANSI/ISA-62443-2-1: Requirements for an IACS Security Management System
- ANSI/ISA-62443-3-2: Security Risk Assessment and System Design
- ANSI/ISA-62443-3-3: System Security Requirements and Security Levels
- ANSI/ISA-62443-4-1: Product Development Requirements
- ANSI/ISA-62443-4-2: Technical Security Requirements for IACS Components

The ISO also addresses cybersecurity. ISO/IEC 27001 is a series of information security management system standards. Similar in concept to ISO 9001 for quality assurance and ISO 14001 for environmental protection, ISO/IEC 27001:2016 provides best practice recommendations on information security management, including privacy, confidentiality,

---

[60] Department of Homeland Security, Critical Manufacturing Sector-Specific Plan, 2015, at https://www.dhs.gov/publication/nipp-ssp-critical-manufacturing-2015.

[61] Interview with Carol Hawk, Program Manager for Cybersecurity for Energy Delivery Systems.

[62] http://isa99.isa.org/ISA99%20Wiki/Home.aspx.

and cybersecurity. Examples of published standards in the ISO/IEC 27001 series include:

- ISO/IEC 27010: Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27019: Information security for process control in the energy industry
- ISO/IEC 27032: Guidelines for cybersecurity
- ISO/IEC 27033: Network security
- ISO/IEC 27035: Information security incident management

Although ISO/IEC 27001 does not specifically target manufacturers, the series includes sufficient detail to provide the basis for a certification program, similar to ISO 9001 quality systems, that could become an integral part of the cultural change needed in industry to increase focus on cybersecurity.

APPENDIX 2

GLOSSARY

Blockchain—A blockchain is a distributed database used to maintain a continuously growing list of records, or blocks. Each block includes a timestamp and a link to a previous block. The data in any given block cannot be altered without altering all subsequent blocks, creating an extremely secure, verifiable database.

Cyberattack—An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Physical Systems (CPS)—Smart systems that include engineered interacting networks of physical and computational components. Cyber physical systems integrate computation, communication, sensing, and actuation with physical systems to fulfill time-sensitive functions with varying degrees of interaction with the environment, including human interaction.

Cybersecurity—The ability to protect or defend the use of cyberspace from cyberattacks.

Cyberspace—A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyber Supply Chain Security—(1) The ability to validate the qualifications (properties, structure, chain of custody, manufactured conditions) of a product or material from a supplier; (2) the ability to validate that data about a product qualification; (3) the ability to protect or defend the use of interconnected cross company cyberspaces from cyberattacks that result in loss or corruption of data about a product or material, change or corruption of data that would alter the expected product output of a manufacturing operation and/or taking over any actuator control of a physical operation.

Cyber Supply Chain Security Resilience—The ability for a supply chain to continue to operate as interconnected cyber space systems while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack.

Data Integrity—The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

Data Security—Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Enterprise Resource Planning (ERP) System—A system that integrates enterprise-wide information including human resources, financials, manufacturing, and distribution as well as connects the organization to its customers and suppliers.

Firewall—An inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance) that forwards or rejects/drops packets on a network. Typically, firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

Information Security—The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Information System—A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Resilience—The ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack.

Information Technology (IT)—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Industrial Control Systems (ICS)—ICS encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

Machine Controller—A control system/motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage.

Malware—Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code (malware).

Manufacturing Execution System (MES)—A system that uses network computing to automate production control and process automation. By downloading recipes and work schedules and uploading production results, a MES bridges the gap between business and plant-floor or process-control systems.

Network—Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Operating System—An integrated collection of service routines for supervising the sequencing of programs by a computer. An operating system may perform the functions of input/output control, resource scheduling, and data management. It provides application programs with the fundamental commands for controlling the computer. Common operating systems are Microsoft Windows, Apple OSX, and Linux.

Operations Technology (OT)—Any physical operating equipment at any level of manufacturing abstraction that is connected within the cyberspace defined by the role of the equipment at that level of abstraction.

Process Controller—A type of computer system, typically rack-mounted, that processes sensor input, executes control algorithms, and computes actuator outputs.

Programmable Logic Controller (PLC)—A small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, switches, and mechanical timer/counters). PLCs have evolved into controllers with the capability of controlling complex processes, and they are used substantially in SCADA systems and DCS. PLCs are also used as the primary controller in smaller system configurations. PLCs are used extensively in almost all industrial processes.

Supervisory Control and Data Acquisition (SCADA)—A generic name for a computerized system that gathers and processes data and applies operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwaves, and satellites.

Trust Anchor—An authoritative entity represented by a public key and associated data. The public key is used to verify digital signatures, and the associated data are used to constrain the types of information or actions for which the trust anchor is authoritative.

APPENDIX 3

CONTRIBUTORS

Sean Atkinson, Global IT Compliance Manager, GLOBALFOUNDRIES

Kristen Baldwin, Acting Deputy Assistant Secretary of Defense for Systems Engineering, Department of Defense

Matt Blaze, Associate Professor of Computer and Information Science (CIS), University of Pennsylvania

Glenn Bleiler, IT Director of Science, Manufacturing, Engineering Technology & Emerging Innovations, Corning

Shaunak Bopardikar, United Technologies Research Center

Benjamin Collar, Head of Cyber Security for the Americas, Siemens

David Corman, Program Director, Division of Computer and Network Systems (CISE/CNS), National Science Foundation

Eric Cosman, Principal Consultant, OIT Concepts LLC

Darren Curtis, Office of Cooperative Threat Reduction, Department of State

Jim Davis, Vice Provost of Information Technology and co-PI, Clean Energy Smart Manufacturing Innovation Institute, UCLA

Trish DiGiacomo, Director, Lab, Manufacturing and Distribution Security & Risk Management, Johnson & Johnson

John Everett, Program Manager, DARPA Information Innovation Office

Kim Finnigan, Government Relations, Regulatory Affairs & Strategic Initiatives, GLOBALFOUNDRIES

Robert Frazier, Chief Security Architect, Lockheed Martin

Kevin Fu, Associate Professor, University of Michigan

Sam Fuller, CTO emeritus, Analog Devices

Steve Gleason, Cyber Security Director, Micro Craft Inc.

Andre Gudger, Eccalon

Carl Gunter, Professor, University of Illinois

Greg Hager, Mandell Bellmore Professor of Computer Science, The Johns Hopkins University

Vasant Honavar, Professor, Pennsylvania State University

Ken Hoyme, Director of Product Security, Boston Scientific

Mimi Hsu, Lockheed Martin

Rob Ivester, Deputy Director of the Advanced Manufacturing Office (AMO), Office of Energy Efficiency and Renewable Energy (EERE), Department of Energy

Daniel Janisch, Engineering Director, Corning

Larry John, Principal Analyst, ANSER

Anupam Joshi, Director, UMBC Center for Cybersecurity Professor; Chair, Computer Science and Electrical Engineering, University of Maryland, Baltimore County

Kate Klemic, Research Scientist, Virginia Institute of Technology to Virginia Polytechnic Institute and State University Applied Research Corporation

Bruce Kramer, Senior Advisor, National Science Foundation

Kenneth Krieg, Principal, Samford Global Strategies

Lee Lane, Chief Product Security Officer, Rockwell Automation

John Main, Program Manager, Defense Sciences Office, DARPA

Brynne McCord, Senior Program Manager, OSD Manufacturing Technology, Engility

Thomas McDermott, Executive Director, Digital Manufacturing and Design Innovation Institute (DMDII)

Michael McGrath, Principal Consultant, McGrath Analytics LLC

Beth Mynatt, Professor, Georgia Institute of Technology

Richard Naylor, Senior Cyber Advisor & Deputy Director Counter Intelligence, Defense Security Service, Department of Defense

Amanda Needham, Manager of Program Design, Digital Manufacturing and Design Innovation Institute (DMDII)

Sandeep Neema, Program Manager, DARPA Information Innovation Office

Andrew Nord, Office of Cooperative Threat Reduction, Department of State

Dennis Pollutro, Director of Strategic Initiatives, Intelligent Decisions

Adam Porter, Executive Director, Fraunhofer USA

Greg Purdy, Research Assistant Professor, Virginia Institute of Technology to Virginia Polytechnic Institute and State University Applied Research Corporation

Sudarsan Rachuri, Program Manager of CESMII, Department of Energy

Adele Ratcliff, Director of the DOD Manufacturing Technology (ManTech) Program, Manufacturing and Industrial Base Policy (MIBP), Department of Defense

Melinda Reed, Deputy Director for Program Protection, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Department of Defense

Ben Richardson, Deputy Director, Industrial Base Protection & Exploitation, Office of the Under Secretary of Defense for Intelligence, Department of Defense

Dan Rozinski, Manufacturing Technology Fellow, Dow Chemical

John Russell, Manufacturing Technology Fellow, National Science Foundation

Mike Russo, Director and Corporate Lead, U.S. Government Affairs, GLOBALFOUNDRIES

Brian Schott, CTO, Nimbis Services

Vyas Sekar, Assistant Professor, CyLab, Carnegie Mellon University

Scott Tousley, Deputy Director, Cyber Security R&D, Department of Homeland Security, Science & Technology

Charles Wessner, Research Professor of Practice, Georgetown University

Dan Wolf, President/CEO, Cyber Pack Ventures, Inc.

Melinda Woods, Defense Production Act Title III Program Director, Office of the Secretary of Defense, Department of Defense

Thorsten Wuest, Assistant Professor, West Virginia University

Fen Zhao, Program Coordinator for the Secure and Trustworthy Cyberspace Program, National Science Foundation

John Zurcher, Program Manager of Federal Critical Infrastructure Assessments, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Department of Homeland Security

APPENDIX 4

WORKSHOP AGENDA

CYBERSECURITY FOR MANUFACTURERS: SECURING THE DIGITIZED AND CONNECTED FACTORY

TUESDAY, MARCH 14
Westin Arlington Gateway, Arlington, VA

8:00 AM	**Check-in Begins,** *F. Scott Fitzgerald DE – 2nd floor*
8:30 AM	**Keynote: Kenneth Krieg –** former Under Secretary of Defense for Acquisition, Technology and Logistics
9:00 AM	**Introductions**
9:30 AM	**CCC, MForesight, Expected Outcomes**
9:45 AM	**Key Challenges**
10:00 AM	**Break**

SESSION 1: DEFINE THE PROBLEMS

10:15 AM **Breakout 1:** Break down key challenges into specific needs and prioritize. Output a list of group's top priority needs to be addressed.

- **A. System level security and cyber-resilience**
- **B. Integrity of manufacturing goods from design to the factory floor**
- **C. Machine-to-machine security, especially legacy systems**
- **D. Securely connecting the factory to the supply chain**

11:15 AM	**Group Outputs and Discussion**
12:00 PM	**Lunch and Networking,** *Pinzimini Dining Room 1 & 2 – 1st floor*

SESSION 2: IDENTIFY SOLUTIONS AND ACTION ITEMS

1:30 PM	**Priority R&D and Implementation Gaps to Address**
1:45 PM	**Breakout 2:** Explore potential solutions to fill gaps. Recommend and prioritize action items to realize solutions. Output key recommendations to be presented in discussion.
2:45 PM	**Break**
3:00 PM	**Breakout 3:** Repeat Breakout 2 for a different gap.
4:00 PM	**Recommendations and Discussion**

WEDNESDAY, MARCH 15
Westin Arlington Gateway, Arlington, VA

SESSION 3: CYBER INTELLIGENCE

8:30 AM	**Today's Objectives,** *F. Scott Fitzgerald DE – 2nd floor*
8:40 AM	**Key Challenges:** André Gudger – former Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy

9:00 AM **Breakout 4:** Define specific needs associated with the challenge. Begin to recommend and prioritize action items to realize solutions. Challenges:

- **A. Intelligence gathering: privacy, security, and efficiency**
- **B. Intelligence and adversary assessment**
- **C. Intelligence sharing in the supply chain**

10:00 AM	**Break**
10:15 AM	**Breakout 4 continued:** Finalize prioritization of action items and prepare recommendations to be presented in discussion.
11:00 AM	**Recommendations, Discussion and Next Steps**
11:55 AM	**Closing Remarks and Evaluations**
12:00 AM	**Box Lunch and Networking**

REFERENCES

Aeppel, Timothy. "Old Machines Show Why Trump Tax Breaks May Not Spark New Company Spending," *Reuters,* May 19, 2017, at http://www.reuters.com/article/us-usa-manufacturing-investment-analysis-idUSKCN18E1DI.

Aon. *2017 Global Risk Management Survey,* at http://www.aon.com/2017-global-risk-management-survey/index.html.

Barlyn, S. and C. Cohn. "Companies Use Kidnap Insurance to Guard Against Ransomware Attacks," *Reuters,* May 19, 2017, at http://www.reuters.com/article/cyber-attack-insurance-idUSL2N1IL1OL.

Bayer, T. et al. "An Operations Concept for Integrated Model-Centric Engineering at JPL," Paper #1120 IEEE Aerospace Conference, 6-13 March 2010, DOI:10.1109/AERO.2010.5446799.

BDO, USA, LLP. "Manufacturing Industry Serves Up New Risks," *2016 BDO Manufacturing Riskfactor Report,* at https://www.bdo.com/getattachment/1d428874-8f92-4c85-af58-6bf238530dbe/attachment.aspx?2016-M-D-RiskFactor-Report-Brochure-WEB.pdf.

Belikovetsky, S. M. Yampolskiy, et. al. "Cyber-Physical Attack with Additive Manufacturing," September 2016, at https://arxiv.org/pdf/1609.00133v1.pdf.

Bevan, O., S. Ganguly, et. al. "'The Ghost in the Machine:' Managing Technology Risk," McKinsey & Co., July 2016, at http://www.mckinsey.com/business-functions/risk/our-insights/the-ghost-.

Breunig, M., R. Kelly, et. al. "Getting the Most out of Industry 4.0," April 2016, at http://www.mckinsey.com/business-functions/operations/our-insights/industry-40-looking-beyond-the-initial-hype.

Candell, R., D.M. Anand, and K. Stouffer. "A Cybersecurity Test bed for Industrial Control Systems," Process Control & Safety Symposium 2014, 6-9 October 2014, at https://www.nist.gov/publications/cybersecurity-test bed-industrial-control-systems.

Cayler, P., O. Noterdaeme, and K. Naik. "Digital in Industry: From Buzzword to Value Creation," *Digital McKinsey.* August 2016, at http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-in-industry-from-buzzword-to-value-creation.

Center for Strategic & International Studies. "Significant Cyber Incidents Since 2006," at https://www.csis.org/programs/technology-policy-program/cybersecurity/other-projects-cybersecurity/significant-cyber.

Cisco. 2017 *Annual Cybersecurity Report.* San Jose, CA: Cisco Systems, Inc. 2017, at http://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Committee on 21st Century Cyber-Physical Systems Education. *A 21st Century Cyber-Physical Systems Education.* Washington, D.C.: National Academies Press, 2016.

Cornford, S., et al. "Evaluating a Fractionated Spacecraft System: A Business Case Tool for DARPA's F6 Program," IEEE Aerospace Conference, 3-10 March 2012, DOI:10.1109/AERO.2012.6187435.

Cyber Physical Systems Public Working Group. *Framework for Cyber-Physical Systems,* Release 1.0, May 2016.

Department of Homeland Security. *Critical Manufacturing Sector-Specific Plan,* 2015 at, https://www.dhs.gov/publication/nipp-ssp-critical-manufacturing-2015.

Geopfert, D. "Manufacturers Pay a Steep Price for Data Vulnerability," *RSM Insight,* January 12, 2017, at http://rsmus.com/what-we-do/industries/industrial-products/manufacturing-insights/manufacturers-pay-a-steep-price-for-data-vulnerability.html.

Huelsman, T., E. Powers, et. al. *Cyber Risk in Advanced Manufacturing.* Deloitte Center for Industry Insights and the Manufacturers Alliance for Productivity and Innovation, 2016, at www2.deloitte.com/content/dam/../us-manu-cyber-risk-in-advanced-manufacturing.pdf.

ISA99 Committee. *ISA99: Developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security,* at http://isa99.isa.org/ISA99 Wiki/Home.aspx.

Honeywell International. "Mitigating Cyber Security Risks in Legacy Process Control Systems," November 2014, at https://www.honeywellprocess.com/en-US/online_campaigns/IndustrialCyberSecurity/Pages/latest-news2.html.

Industrial Control Systems Emergency Response Team, Advanced Analytical Laboratory. *Malware Trends.* Department of Homeland Security. October 2016, at https://ics-cert.us-cert.gov/sites/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper_S508C.pdf.

Industrial Internet Consortium. *Industrial Internet of Things Volume G1: Reference Architecture,* 2017, at http://www.iiconsortium.org/IIRA.htm.

Industrial Internet Consortium. *Industrial Internet of Things Volume G4: Security Framework,* 2016, at http://www.iiconsortium.org/IISF.htm.

Finkle, J., "Security firms warn of new cyber threat to electric grid," *Reuters,* June 12, 2017, at http://www.reuters.com/article/us-cyber-attack-utilities-idUSKBN1931EG.

IBM Managed Security Services. *Security Attacks on Industrial Control Systems: How Technology Advances Create Risks for Industrial Organizations.* October 2015, at https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-4573&S_PKG= ov39538.

IBM Managed Security Services. *Security Trends in the Manufacturing Industry: Targeting Control Systems and Crown Jewels.* January 2016, at https://securityintelligence.com/media/security-trends-in-the-manufacturing-industry/.

Imprimis, Inc. *Summary of Changes and Requirements—DFARS Cybersecurity Safeguards,* Colorado Springs, CO: Imprimis, Inc., 2017, at http://docs.wixstatic.com/ugd/ce99b5_cd8da1b5c63c4cab81126327a84bf46d.pdf.

Kirk, J. "Second variant of Stuxnet worm strikes," *InfoWorld,* July 20, 2010, at http://www.infoworld.com/article/2625596/endpoint-protection/second-variant-of-stuxnet-worm-strikes.html.

Kumar, M. "Irongate—New Stuxnet-like Malware Targets Industrial Control Systems," *The Hacker News,* June 4, 2016, at http://thehackernews.com/2016/06/irongate-stuxnet-malware.html.

Long, J. "Model-Based Systems Engineering for Project Success: The Complete Process," INCOSE International Symposium, 20: 1502–1644. (2010) doi: 10.1002/j.2334-5837.2010.tb01154.x.

Long, M. "Stuxnet Strike on U.S. Utility Signals Disturbing Trend," *Yahoo News,* Nov. 21, 2011, at https://www.yahoo.com/news/stuxnet-strike-u-utility-signals-disturbing-trend-224036723.html.

Mahoney, T. and S. Helper. *Ensuring American Manufacturing Leadership Through Next Generation Supply Chains,* MForesight: Alliance for Manufacturing Foresight, June 2017, at http://mforesight.org.

McMillen, D. "Attacks Targeting Industrial Control Systems Up 110 Percent," *Security Intelligence,* December 27, 2016, at https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent.

Moyer, H. and C. Rieger. "Cybersecurity for Advanced Manufacturing," presentation at National Defense Industries Association Cybersecurity for Advanced Manufacturing Forum, Arlington, VA, November 15, 2016.

Nakashima, E. and S. Mufson. "U.S., China vow not to engage in economic cyber espionage," *The Washington Post,* September 25, 2015, at https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html?utm_term=.4a1b98dbfaab.

National Council of ISACs. "Member ISACs," at https://www.nationalisacs.org/member-isacs.

National Institute of Standards and Technology. *Baldrige Cybersecurity Excellence Builder,* version 1.0, March 2017, at https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity,* Draft version 1.1, January 10, 2017.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. *Report of the Defense Science Board Task Force on Cyber Supply Chains,* Washington, D.C.: February 2017.

PriceWaterhouseCooper. "Toward New Possibilities in Threat Management," *Key Findings From Global State of Information Security Survey 2017,* at http://www.pwc.com/gsiss.

Rachuri, Sudarsan. Presentation at Clean Energy Smart Manufacturing Innovation Institute, February 2017, at https://www.cesmii.org/s/CESMII-Kickoff-Sudarsan-Rachuri-DOE.pdf.

Raymond, Brian. *"What Makes the Manufacturing Sector Unique," in The Cybersecurity Social Contract.* Washington, D.C.: Internet Security Alliance, 2016, pp. 155-162, at http://www.nam.org/Issues/Technology/Cybersecurity/.

Rockwell Automation. *Industrial Security: Protecting Networks and Facilities Against a Fast-Changing Threat Landscape.* July 2016, at http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/secur-wp004_-en-e.pdf.

Ross, R., M. McEvilley, and J. Oren. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* NIST Special Publication 800-160, November 2016, at https://doi.org/10.6028/NIST.SP.800-160.

Ross, R., P. Viscuso, G. Guissanie, et. al. *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,* NIST Special Publication 800-171, June 2015, at http://dx.doi.org/10.6028/NIST.SP.800-171.

Sandia National Laboratories. *National Supervisory Control and Data Acquisition (SCADA) Test Bed,* at http://energy.sandia.gov/energy/ssrei/gridmod/cyber-security-for-electric-infrastructure/scada-systems/.

Schwiters, N. and B. Moritz. "10 Principles for Leading the Next Industrial Revolution," *Strategy + Business,* March 23, 2017, at https://www.strategy-business.com/article/10-Principles-for-Leading-the-Next-Industrial-Revolution?gko=f73d3.

Shrobe, H. "Cybersecurity," excerpt from *The Future Postponed: Why Declining Investment in Basic Research Threatens a U.S. Innovation Deficit.* Cambridge, MA: Massachusetts Institute of Technology, 2015.

Simpson, A. "Increasing the Potential of IoT Through Security and Transparency," Department of Commerce, National Telecommunications and Information Administration, August 2, 2016, at https://www.ntia.doc.gov/blog/2016/increasing-potential-iot-through-security-and-transparency.

Stouffer, K., and J. McCarthy. *Securing Manufacturing Industrial Control Systems: Cybersecurity for Manufacturing,* NIST National Cybersecurity Center of Excellence, March 2017, at https://nccoe.nist.gov/projects/use-cases/capabilities-assessment-securing-manufacturing-industrial-control-systems.

Stouffer, K., V. Pillitteri, et. al. *Guide to Industrial Control Systems (ICS) Security,* NIST Special Publication 800-82 Revision 2, May 2015, at http://dx.doi.org/10.6028/NIST.SP.800-82.

"Stuxnet Variant Discovered in European Systems," *Power,* Oct. 19, 2011, at http://www.powermag.com/stuxnet-variant-discovered-in-european-systems/.

Symantec. *Internet Security Threat Report,* April 2017, at https://www.symantec.com/security-center/threat-report.

Symantec. *Smarter Security for Manufacturing in the Industry 4.0 Era.* 2016, at https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf.

Trend Micro, *TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats.* 2017, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup.

MFORESIGHT
ALLIANCE FOR MANUFACTURING FORESIGHT

www.mforesight.org