Journal of Manufacturing Systems xxx (2018) xxx–xxx

Contents lists available at ScienceDirect

Journal of Manufacturing Systems

journal homepage: www.elsevier.com/locate/jmansys

Cybersecurity for digital manufacturing

Dazhong Wu[a,*], Anqi Ren[b], Wenhui Zhang[c], Feifei Fan[d], Peng Liu[c], Xinwen Fu[e], Janis Terpenny[b]

[a] Department of Mechanical and Aerospace Engineering, University of Central Florida, Orlando, FL 32816, USA
[b] Department of Industrial and Manufacturing Engineering, Pennsylvania State University, University Park, PA 16802, USA
[c] College of Information Sciences and Technology, Pennsylvania State University, University Park, PA 16802, USA
[d] Department of Mechanical Engineering, University of Nevada, Reno, NV 89557, USA
[e] Department of Computer Science, University of Central Florida, Orlando, FL 32816, USA

ARTICLE INFO

Article history:
Received 4 December 2017
Received in revised form 7 March 2018
Accepted 14 March 2018
Available online xxx

Keywords:
Cybersecurity
Threat and vulnerability assessment
Control methods
Industrial Internet of Things
Digital manufacturing

ABSTRACT

Digital manufacturing aims to create highly customizable products with higher quality and lower costs by integrating Industrial Internet of Things, big data analytics, cloud computing, and advanced robots into manufacturing plants. As manufacturing machines are increasingly retrofitted with sensors as well as connected via wireless networks or wired Ethernet, digital manufacturing systems are becoming more accessible than ever. While advancement in sensing, artificial intelligence, and wireless technologies enables a paradigm shift in manufacturing, cyber-attacks pose significant threats to the manufacturing sector. This paper presents a review of cybersecurity in digital manufacturing systems from system characterization, threat and vulnerability identification, control, and risk determination aspects as well as identifies challenges and future work.

© 2018 Published by Elsevier Ltd on behalf of The Society of Manufacturing Engineers.

1. Introduction

Digital manufacturing refers to a manufacturing paradigm that aims to make use of Industrial Internet of Things (IIoT), cloud computing, artificial intelligence or machine learning, advanced robotics to improve manufacturing productivity and cost efficiency [1–3]. As one of the key enabling technologies for digital manufacturing, cloud-based manufacturing refers to a service-oriented manufacturing paradigm in which service consumers perform design and manufacturing tasks using cloud-based digital design, engineering analysis, manufacturing applications [4]. Manufacturing service providers offer manufacturing services through various service delivery models such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), Hardware-as-a-Service (HaaS), and Maintenance-as-a-Service (MaaS) [5–8]. For example, IaaS provides users with computing and network resources such as high performance servers, cloud storage, and wireless networks. PaaS provides a development environment or a platform that allow users to develop and manage cloud-based applications without building and maintaining the infrastructure. SaaS provides access to cloud-based computer-aided design (CAD), computer-aided engineering (CAE) or finite element analysis (FEA), and computer-aided manufacturing (CAM) software over the Internet. HaaS enables manufacturers to scale up manufacturing capacity by renting manufacturing resources such as lathes, milling machines, and 3D printers from service providers. MaaS provides manufacturers with manufacturing process monitoring and predictive maintenance services that predict manufacturing equipment malfunctions, improve product quality and process reliability, and prevent unplanned machine downtime.

While IIoT, cloud computing, artificial intelligence are driving innovation in the manufacturing sector, manufacturers are increasingly vulnerable to cyber-attacks [9–18]. According to a report by Accenture and the Ponemon Institute [19], the average cost of cyber-crime globally reached $11.7 million per organization in 2017. Cyber threats have evolved from targeting computers, networks, smartphones, and power grids to the manufacturing sector due to a lack of investment in cybersecurity. According to NBC News, the manufacturing sector in the U.S. lost nearly $240 billion in revenue and 42,220 manufacturing jobs from 2002 to 2012 due to cyber-attacks [20]. One of the primary reasons why the manufacturing sector is among one of the most frequently hacked industries, second only to healthcare, is largely due to IIoT-connected machines, cloud-based remote sensing and control systems. For example, Stuxnet, a malicious computer worm first discovered in 2010, was created to target supervisory control and data acquisition (SCADA) systems and programmable logic con-

[*] Corresponding author.
E-mail address: dazhong.wu@ucf.edu (D. Wu).

https://doi.org/10.1016/j.jmsy.2018.03.006
0278-6125/© 2018 Published by Elsevier Ltd on behalf of The Society of Manufacturing Engineers.

trollers (PLCs) [21–23]. Stuxnet destroyed almost one fifth of Iran's nuclear centrifuges by infecting over 200,000 computers and causing 1000 machines to physically degrade. In 2014, attackers hacked the control system of a German steel factory using booby-trapped emails. A report by the Federal Office for Information Security [24] revealed that the control system was not able to shut down a blast furnace properly due to this cyber-attack.

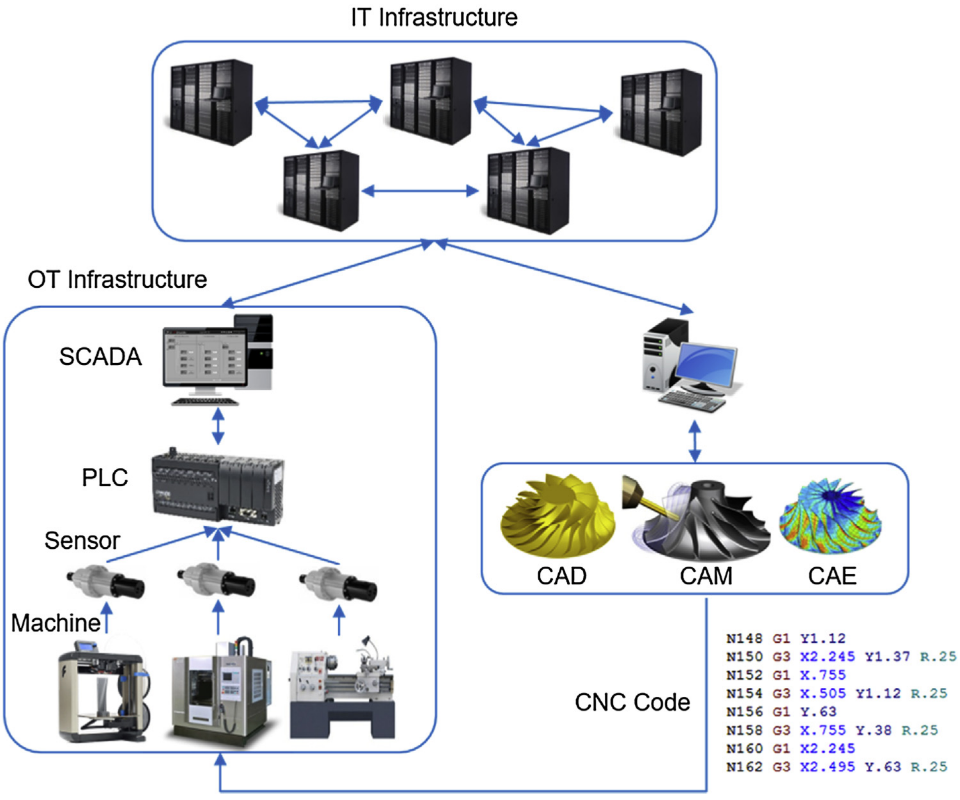
According to a recent report by Trend Micro, a cybersecurity research team demonstrated how cyberattacks on an industrial robot from ABB can be successfully executed [25]. In the first attack, the attacker altered the control system of the industrial robot so that the robot moves inaccurately. This attack resulted in defective parts. In the second attack, the attacker changed the calibration parameters of the robot, reducing the positioning accuracy of the robot significantly. In the third attack, the attacker manipulated the program used by the robot, introducing defects in a workpiece. In the fourth attack, the attacker manipulated the status information of the robot. This attack may result in operator injuries. In addition to the threats unique to manufacturers, the manufacturing industry is also facing a variety of prevalent cyber-attack techniques such as malware. According to the U.S. National Center for Manufacturing Science (NCMS), variants of Trojans and droppers accounted for 86% of the malware in the manufacturing sector [26].

The most important security goal is protecting confidentiality, integrity, and availability (also known as CIA triad) of data. Confidentiality involves preventing sensitive data and information from being disclosed to unauthorized parties. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data. Availability involves keeping data and resources available for authorized use. According to the National Institute of Standards and Technology (NIST), a risk assessment methodology consists of system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, and control recommendations. In addition, NIST developed a systematic cybersecurity framework as well as identified a few cybersecurity objectives for manufacturing [27]. The five functions of the framework include identify, protect, detect, respond, and recover. This paper presents a review of cybersecurity in digital manufacturing systems from system characterization, threat and vulnerability identification, control, and risk determination aspects.

The remainder of this paper is organized as follows: Section 2 presents the boundaries of digital manufacturing systems. Section 3 identifies threats and system vulnerabilities that could be exploited by potential threat-sources as well as presents two attack scenarios. Section 4 discusses control methods that could be implemented to minimize the likelihood of a threat's exercising a system vulnerability. Section 5 presents the quantitative methods that assess the level of risk to manufacturing systems. Section 6 discusses challenges and future work for addressing cybersecurity issues in digital manufacturing.

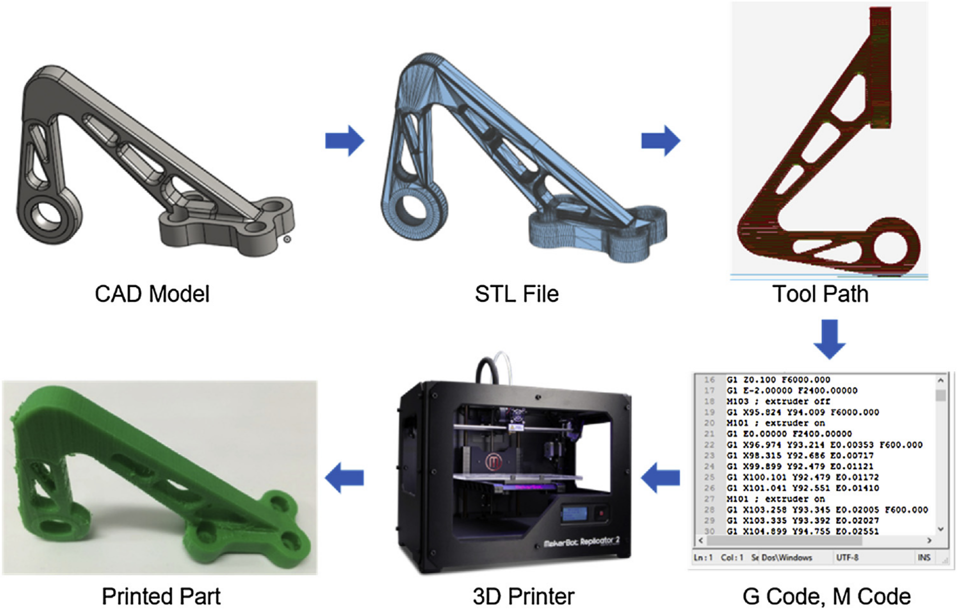
2. System characterization

To assess risks for a manufacturing system, the first step is to identify the components, resources, and information that constitute the system. A manufacturing system consists of five layers, including enterprise resource planning (ERP) systems, manufacturing execution systems (MES), SCADA and PLCs, sensors and actuators, and industrial protocols. A manufacturing execution system is a control system that improves productivity and reduces cycle time by monitoring and controlling manufacturing machines in real time. A SCADA system consists of supervisory computers, remote terminal units, PLCs, communication infrastructure, and a human-machine interface. A SCADA system gathers data on manufacturing processes from PLCs, sensors, and actuators as well as sends control commands to the field connected devices. PLCs perform sequential relay control, motion control, and process control.



```
N148 G1 Y1.12
N150 G3 X2.245 Y1.37 R.25
N152 G1 X.755
N154 G3 X.505 Y1.12 R.25
N156 G1 Y.63
N158 G3 X.755 Y.38 R.25
N160 G1 X2.245
N162 G3 X2.495 Y.63 R.25
```

Fig. 1. Manufacturing system model.



```
G1 Z0.100 F6000.000
G1 E-2.00000 F2400.00000
M103 ; extruder off
G1 X95.824 Y94.009 F6000.000
M101 ; extruder on
G1 E0.00000 F2400.00000
G1 X96.974 Y93.214 E0.00353 F600.000
G1 X98.315 Y92.686 E0.00717
G1 X99.899 Y92.479 E0.01121
G1 X100.101 Y92.479 E0.01172
G1 X101.041 Y92.551 E0.01410
M101 ; extruder on
G1 X103.258 Y93.345 E0.02005 F600.000
G1 X103.335 Y93.392 E0.02027
G1 X104.899 Y94.755 E0.02551
```

Fig. 2. A workflow of computer-aided additive manufacturing.

PLCs have built-in communications ports (e.g., RS-232, RS-422, RS-485, and Ethernet) that receive inputs from status components (e.g., sensors and switches). Some of the most common industrial protocols include Modbus, Profibus, EtherNet/IP, MTConnect, and OPC Unified Architecture (OPC UA). To secure a manufacturing system, software, hardware, operating systems or firmware, network, and data security should be considered.

Fig. 1 illustrates a digital manufacturing system model consisting of information technology (IT) and operational technology (OT) systems. The IT systems use computers to store, retrieve, transmit, and process design- and manufacturing-related data such as CAD models and CNC programs. The OT systems use hardware (e.g., sensors and PLC) and software (e.g., SCADA) to monitor and control manufacturing equipment (e.g., valves and pumps) and manufacturing processes (e.g., milling and turning). With the emergence of the IIoT technologies, IT systems used for data-intensive computing has been integrated with OT systems used to monitor and control events, processes, and devices.

Fig. 2 illustrates an example workflow of computer-aided additive manufacturing processes. First, a CAD model that contains all the geometric information of a part is created using CAD tools. Second, the CAD model is converted into a standard triangle language (STL) file which is supported by almost all the CAD software packages. An STL file describes a raw unstructured triangulated surface (also known as facet) by the unit normal and vertices of the triangles. Third, the digital model is sliced into thin layers, and a toolpath is generated using G-code and M-code. The toolpath file contains the commands that control the motion of an actuator. Last, the part is printed on a 3D printer.

3. Threat and vulnerability identification

After characterizing a manufacturing system, the next step is to identify threats and vulnerabilities. According to the NIST's risk management guide for information technology systems [28], a threat refers to "the potential for a particular threat-source to successfully exercise a particular vulnerability." A threat source refers to "any circumstance or event with the potential to cause harm to an IT system." A vulnerability refers to "a flaw or weakness in system security procedures, design, implementation, or internal controls that could result in a security breach or a violation of systems' security policy." An attack refers to "an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity." Table 1 summaries a list of vulnerability/threat pairs.

Table 2 summaries a list of potential attacks on digital manufacturing systems and consequences. An access attack is the act of gaining untheorized access to a network, a system, an application software or other resources without permission. Access attacks include password attacks, trust exploitation, and port redirection. A typical consequence of access attacks is loss of confidential information. In the context of manufacturing, attackers could gain unauthorized access to sensitive systems (e.g., product data management systems) and data (e.g., CAD/CAM files). A denial-of-service attack refers to a cyber-attack where hardware, software, or critical infrastructures are made unavailable to intended users by temporarily or indefinitely disrupting normal operations. In the context of manufacturing, attackers could disrupt cloud computing services for data-intensive applications. A Man-in-the-Middle attack refers to an attack where attackers relay and alter messages between SCADA systems and machines. Malicious software (also known as malware) include Trojans, computer viruses, worms, ransomware, and spyware. Data manipulation refers to the practice of altering digital documents rather than stealing data and holding it for ransom. In the context of manufacturing, attackers could change part dimensions in CAD files or manufacturing process parameters such as speed and temperature in CNC programs. Changing these data could result in physical damages to manufacturing machines, poor product quality, and operator injury or death.

To identify cyber threats and potential vulnerabilities, it is important to develop attack scenarios and understand potential cyber-attacks before they happen. In Sections 3.1 and 3.2, two cyber-attack scenarios that could cause product quality problems are presented.

3.1. Attack scenario 1: changing the CAD model of a part

As shown in Figs. 1 and 2, a typical digital manufacturing process includes CAD, FEA, and CAM. In the CAD and FEA phases, design engineers develop an optimal product design (e.g., dimension,

Table 1
Vulnerability/threat pairs [28].

Target	Vulnerability	Threat-Source
Software	Input validation, privilege escalation, software coding vulnerabilities	Hacker, cracker, computer criminal, terrorist, industrial espionage, insiders, governments
Hardware	Malicious logic, open debugging ports	Insiders
Operating systems or firmware	Unpatched systems, vulnerable system components	Hacker, cracker, computer criminal, terrorist, industrial espionage, insiders, governments
Network	Limited bandwidth susceptible to jamming, unencrypted communication, weak network security protocols such as authentication	Hacker, cracker, computer criminal, terrorist, industrial espionage, insiders, governments
Data	Plaintext with no encryption, no message integrity code (MAC)	Hacker, cracker, computer criminal, terrorist, industrial espionage, insiders, governments

Table 2
A list of potential attacks on digital manufacturing systems.

Attack	Method	Consequence
Access attacks (e.g., Password attacks, Trust exploitation, Port scan)	Gain unauthorized access to a network, a system, an application software, or other resources	Loss of confidential information
Denial-of-Service (DoS) and service delay	Make hardware, software, or infrastructure unavailable to their intended users	Operational disruption, loss of productivity
Man-in-the-Middle (MITM)	Relay and alter messages between machines and remote control systems	Physical damage, poor product quality, injury or death, loss of confidential information
Malicious software (e.g., Trojans, viruses, and worms)	Destroy manufacturing systems by inserting programs with malicious intent onto a manufacturing system	Operational disruption, loss of productivity, Physical damage, poor product quality, injury or death
Data manipulation	Access and change sensitive data such as the key parameters of digital models and documents	Physical damage, poor product quality, injury or death

weight, and material) that satisfies all of the design requirements and constraints, and then create the digital model of the product. In the first attack scenario, attackers could change the geometry parameters of a part by gaining unauthorized access to the CAD model of the part stored in a cloud environment. Assume that the CAD model is stored in Dropbox, one of the most popular cloud storage provider. Dropbox uses secure sockets layer (SSL) transfers for synchronization and stores the data via advanced encryption standard (AES)-256. When a user adds a file to a local Dropbox folder, the Dropbox client application calculates the hash values of all the chunks of the file using the secure hash algorithm (SHA)-256 algorithm. Mulazzani et al. [29] introduced three different attacks on Dropbox that enable unauthorized file access, including hash value manipulation attack, stolen host ID attack, and direct download attack. For example, Dropbox uses OpenSSL, a software library for applications that secure communications over computer networks, to calculate hash values by including a wrapper library called NCrypto. Dropbox does not verify the integrity of the data when dynamically linking to NCrypto. As a result, an attacker could modify the publically available source code of NCrypto so that the hash values can be manipulated. Due to the manipulation of the hash values, the attacker can gain unauthorized access to the files stored in Dropbox without being detected. Once the attacker gains the access to the CAD model of a part, the geometry parameters of a part can be modified. This attack will result in invisible structural defects on critical features. Such a defect can cause product quality degradation with a significantly reduced service life or an unexpected catastrophic failure. For example, a cyber-attack to the CAD model of an engine bracket can degrade the mechanical performance of the bracket. During service, the base of the bracket is mounted to a substrate through bolts, and the bracket carries an external cyclic load.

Fig. 3(a) shows the geometry of the bracket. The material of the bracket is assumed linear elastic (Young's modulus, E, and Poisson's ratio v = 0.35). Fig. 3(b) shows the boundary and loading conditions. Fig. 3(c) presents finite element simulation results of the normalized von Mises stress (σ_e/E) distribution under a load of −p ($p = 1 \times 10^{-4}E$). The stress distribution indicates that the connection area where the beam portion of the bracket meets the base portion is a critical location. This area could be a vulnerable target for cyber-attacks to create structural defects. The defects created in this connection area can result in degradation of mechanical performance. Fig. 4 shows the normalized von Mises stress distribution under a load of −p in the bracket with an invisible elliptic cylinder hole created in the connection region. The maximum von Mises stress increases considerably. As a result, the overall strength of the bracket is significantly reduced. In addition, stress is commonly used to evaluate fatigue life using a stress-life approach. Due to the increase in stress magnitude, the defect can shorten the fatigue life of the bracket.

3.2. Attack scenario 2: changing process parameters in a CNC program

In the second attack scenario, attackers could modify manufacturing process parameters in a CNC program by gaining unauthorized access to the microcontrollers of manufacturing equipment. A CNC program consists of G-code and M-code. G-code is a special programming language that is interpreted by CNC controllers to control the motions of a cutting tool. G-code instructs a cutting tool where to move, how fast to move, and what path to follow. M-code defines program flow and controls auxiliary functions such as coolant, tool change, and spindle rotation.

Fig. 5(a) and (b) shows the CAD model of an engine bracket and the tool path generated by the tool path generator of a 3D printer, respectively. Fig. 6 shows the CNC program generated by the G-code generator of the 3D printer. Changing G01 (linear feed move) could result in incorrect tool paths. Changing G21 could result in incorrect units. Changing M104 S200 could result in over heating or under heating. Changing F7800 could result in an incorrect feed rate.

In this scenario, we take a 3D printer as an example. Attackers may deploy both local physical attacks (for example, executed by insiders) and remote cyberattacks as shown in Fig. 7. Assume

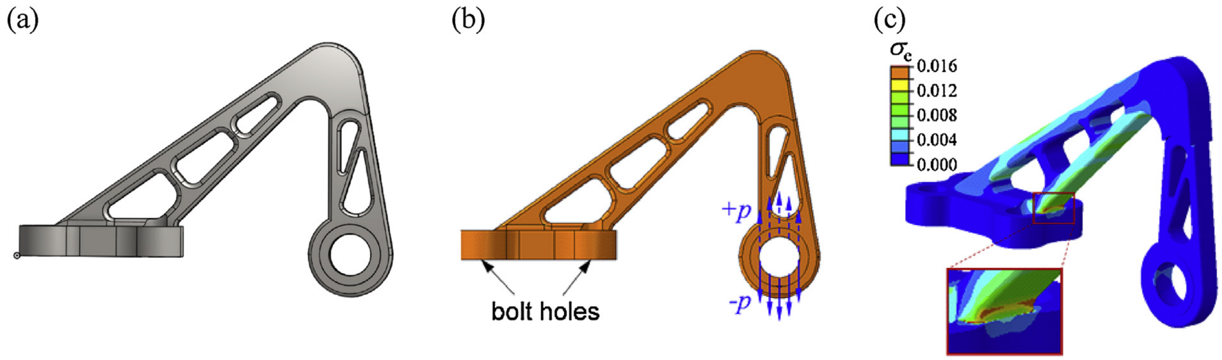


Fig. 3. (a) CAD model; (b) Finite element simulation; (c) Von Mises stress distribution.

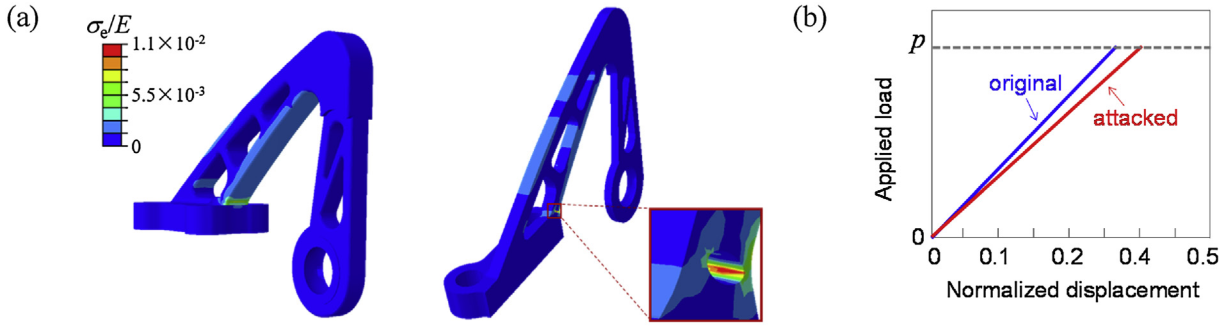


Fig. 4. (a) Finite element results of normalized von Mises stress distribution; (b) Load versus displacement curve.

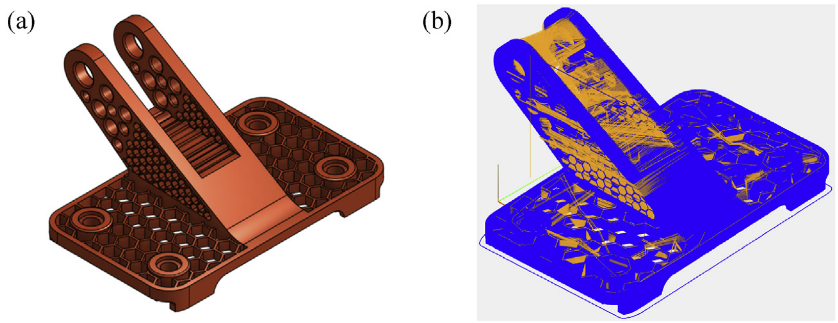
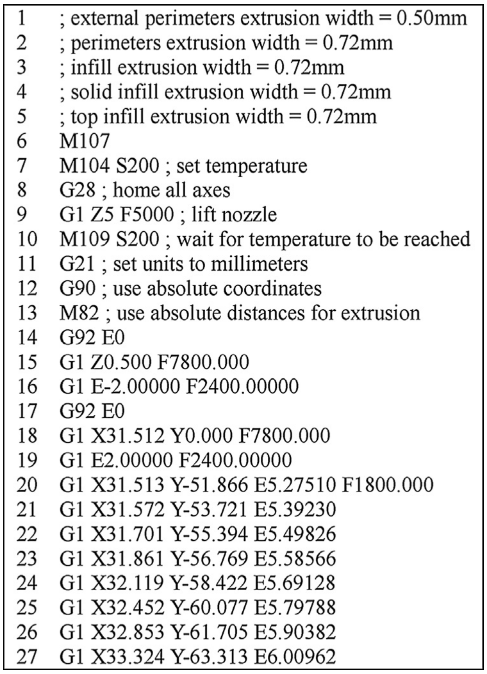


Fig. 5. (a) CAD model; (b) Tool path for printing the engine bracket.

that the microcontroller on the 3D printing is an ATmega chip. ATmega chips are widely used in industry due to its low-power and high-performance features. For example, ATmega1284P is a popular microcontroller. It has 128K bytes On-chip In-System Reprogrammable Flash memory for program storage, which is divided into two sections: application program section and boot program section [30]. It has 16K bytes SRAM data memory, including the register file, standard I/O memory, extended I/O memory and internal data SRAM. In addition, ATmega1284P has 4K bytes EEPROM data memory.

An attacker with physical access to the device with the ATmega1284P controller may deploy a local physical attack. ATmega1284p provides some security mechanisms including on-chip fuses and clocks to mitigate physical attacks. Fuses can be used to configure the ATmega1284P chip. For example, fuses decide whether a boot loader is used, how much memory is used for the boot loader, and disabling serial programming. Some of the fuse bits and lock bits can be used to lock the chip. Programming the fuse and lock bits will add protection to the contents written to flash and EEPROM memories. For example, fuse and lock bits can be used to lock writing and reading to/from FLASH memory (either application or bootloader section). They can be used to lock writing and reading to/from EEPROM memory through JTAG/SPI or other ports. Setting fuse bits can only disable JTAG/SPI port access, but it cannot prevent HVPP (High Voltage Parallel Programming) from reading memory through a programmer board (AVR dragon board). Only Lock bits (LB1, LB2) can disable HVPP. It can be observed that fuse and locks bits must be carefully configured so that an attacker with physical access to the device with the controllers cannot change the flash memory.

A local attack may also be deployed through an insecure boot loader, which runs when the ATmega1284p chip is powered-up or restarted, initializing the device and check for external communication. A boot loader itself can be loaded onto an ATmega1284P chip through the SPI port. ATmega1284P can then use a boot loader to communicate with a connected computer through the UART port to install a new firmware/program to the chip flash. The boot loader can implement encryption and integrity check to protect the content on flash. The boot loader must be password protected so that an attacker with physical access to the device with the controllers



```
; external perimeters extrusion width = 0.50mm
; perimeters extrusion width = 0.72mm
; infill extrusion width = 0.72mm
; solid infill extrusion width = 0.72mm
; top infill extrusion width = 0.72mm
M107
M104 S200 ; set temperature
G28 ; home all axes
G1 Z5 F5000 ; lift nozzle
M109 S200 ; wait for temperature to be reached
G21 ; set units to millimeters
G90 ; use absolute coordinates
M82 ; use absolute distances for extrusion
G92 E0
G1 Z0.500 F7800.000
G1 E-2.00000 F2400.00000
G92 E0
G1 X31.512 Y0.000 F7800.000
G1 E2.00000 F2400.00000
G1 X31.513 Y-51.866 E5.27510 F1800.000
G1 X31.572 Y-53.721 E5.39230
G1 X31.701 Y-55.394 E5.49826
G1 X31.861 Y-56.769 E5.58566
G1 X32.119 Y-58.422 E5.69128
G1 X32.452 Y-60.077 E5.79788
G1 X32.853 Y-61.705 E5.90382
G1 X33.324 Y-63.313 E6.00962
```

Fig. 6. A CNC program.

cannot change the flash memory through the UART port. It can be observed that the bootloader has to be carefully programmed so that an attacker with physical access to the device with the controllers cannot change the flash memory.

An attacker can also deploy remote cyberattacks. A computer can communicate with a controller through the UART port. If the computer is connected to the Internet and has vulnerabilities, the device with the ATmega1284P microcontroller controlled by the computer will be subject to cyberattacks if the computer is compromised. For example, if the bootloader of the microcontroller does not employ passwords or uses weak password, an attacker can control the microcontroller from the compromised computer. This remote attack is similar to Stuxnet, which destroyed almost one fifth of Iran's nuclear centrifuges [21–23].

4. Control methods

After identifying threats and vulnerabilities, the next step is to analyze the controls that could be implemented to eliminate or minimize the probability that the vulnerabilities may be exercised. Security controls are a set of actions that detect, counteract, or minimize security risks. This section focuses on access control, encryption, authentication, and intrusion detection methods.

Table 3
A list of access control methods.

Method	Reference
Role-based access control	[43,44]
Attribute-based access control	[45]
Context-based access control	[46,47]
View-based access control	[41,42]

4.1. *Access control*

Access control is the selective restriction of access to infrastructures and resources. Access control methods can be classified into four categories, including role-based [31–33], attribute-based [34–37], context-based [38–40], and view-based access control [41,42]. Table 3 summarizes a list of access control methods.

Finin et al. [43] investigated the relationship between the Web Ontology Language (OWL) and the Role-Based Access Control (RBAC) model. Two methods were introduced to RBAC in OWL, representing roles as classes and sub-classes in one approach and as attributes in the other approach. Ferrini and Bertino [44] introduced a XACML and OWL-based framework that support RBAC systems. In this framework, the role hierarchy and the constraints were modeled using an OWL ontology. Priebe et al. [45] introduced an approach that simplifies the specification and maintenance of attribute-based access control (ABAC) policies by extending the attribute management with an ontology-based inference facility. Cirio et al. [46] presented an access control system for context-aware environments. In this system, permissions were associated with a set of rules expressed on measurable parameters and were granted to users who can prove compliance with these rules. Corradi et al. [47] developed a context-based access control (CBAC) model that enables users acquire permissions when entering or leaving a specific context. This model allows for dynamic policy modification with no impact on the service code. Montanari et al. [48] introduced a CBAC policy model that treats context as a first-class principle in the specification and enforcement of policies.

4.2. *Encryption*

In cryptography, encryption refers to the process of encoding a message in a way that only authorized parties can access it.

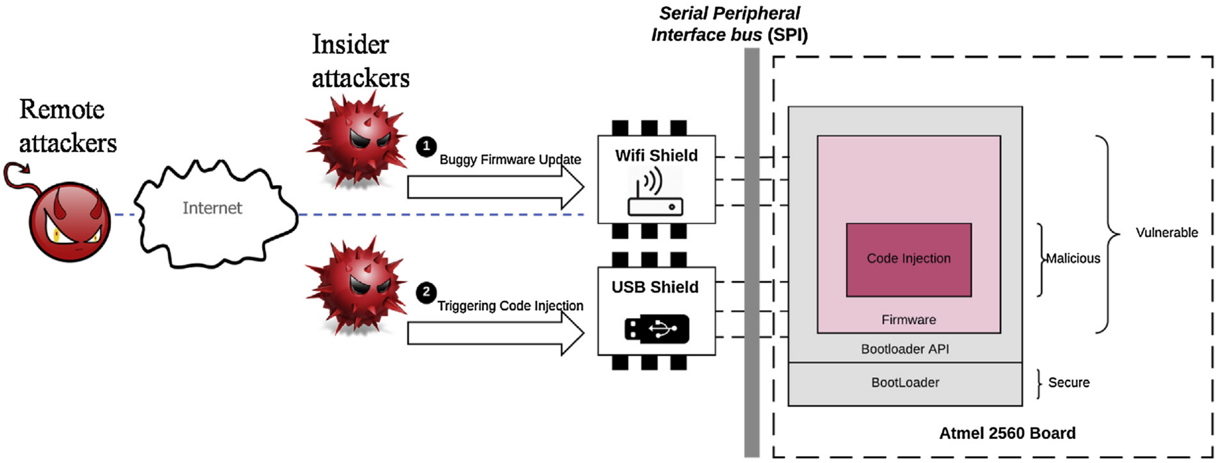


Fig. 7. Threat model.

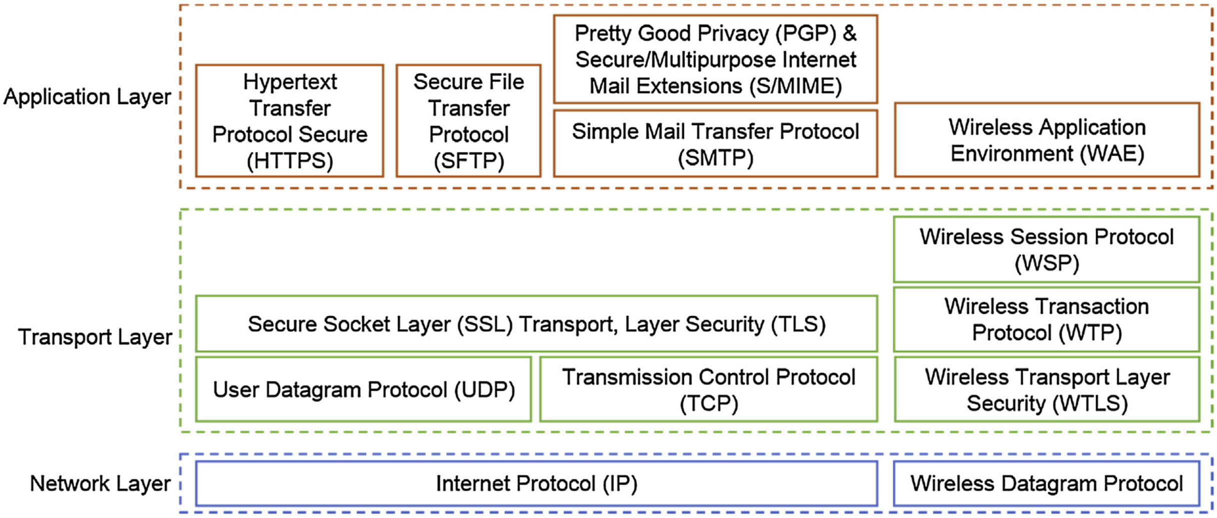

Application Layer
Hypertext Transfer Protocol Secure (HTTPS)
Secure File Transfer Protocol (SFTP)
Pretty Good Privacy (PGP) & Secure/Multipurpose Internet Mail Extensions (S/MIME)
Simple Mail Transfer Protocol (SMTP)
Wireless Application Environment (WAE)
Transport Layer
Wireless Session Protocol (WSP)
Secure Socket Layer (SSL) Transport, Layer Security (TLS)
Wireless Transaction Protocol (WTP)
User Datagram Protocol (UDP)
Transmission Control Protocol (TCP)
Wireless Transport Layer Security (WTLS)
Network Layer
Internet Protocol (IP)
Wireless Datagram Protocol

Fig. 8. Wired Security and Wireless Security Protocols.

Encryption is often implemented in secure communication protocols such as Internet Protocol Security (IPSec), Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), and Wi-Fi Protected Access (WPA). These secure communication protocols support various encryption algorithms. As illustrated in Fig. 8, network secure communication protocols can be classified into three layers, including network, transport, and application layers. At the network layer, IPSec authenticates and encrypts data packets sent over a network. The Triple Data Encryption Algorithm (Triple DEA) is one of the encryption algorithms used by IPSec to encrypt each block of 64 bits of data three times [49]. The services offered by Wireless Data Protocol (WDP) include optional segmentation and reassembly and optional error detection. At the transport layer, transport layer security (TLS) and its predecessor, secure socket layer (SSL), are cryptographic protocols that provide communication security over a computer network. SSL uses various encryption algorithms such as the data encryption standards [50], Triple DEA, and advanced encryption standard [51]. At the application layer, HTTPS is a protocol for authentication of the websites and protection of the privacy and integrity of the exchanged data. HTTPS supports encryption algorithms such as the Rivest-Shamir-Adleman (RSA) algorithm [52] for secure data transmission. SFTP is a network protocol that provides file access, file transfer, and file management over data streams. SFTP supports encryption algorithms such as the Blowfish [53] and Twofish [54] block ciphers. Pretty Good Privacy (PGP) provides cryptographic privacy and authentication for signing, encrypting, and decrypting texts, emails, files, and disk partitions.

4.3. Authentication

Authentication is a process in which the credentials provided are compared to those on file in a database. A user can be authenticated by three factors: what the user knows (memometrics), what the user recognizes (cognometrics), and who the user is (biometrics). In the case of memometrics, a user is authenticated by validating passwords, personal identification numbers (PIN), challenge responses, and security questions. In the case of cognometrics, a user should be able to recognize enrolled items (often out of distractors) presented by a mobile device. This type of authentication mechanism includes various graphical authentication strategies such as Passfaces [55], Déjà Vu [56], and Draw-a-Secret (DAS) [57]. In the case of biometrics, a mobile device stores digitally a person's physiological or behavioral features. The physiological features include fingerprint, retina, iris, face, speaking. The behavioral features include typing dynamics [58,59], mouse clicking patterns [60,61] and signature dynamics [62,63]. In addition, the most commonly used authentication methods fall into three categories: single-factor, two-factor, and multi-factor authentication.

Table 4
Intrusion detection methods.

Category	Method	Reference
Signature-based	State Transition Analysis	[65,66]
	Petri Nets	[67,68]
Anomaly-based	Markov Chain	[69]
	Neural Networks	[70,71]
	Support Vector Machines	[71]
	Decision Tree	[70,72]
	Random Forests	[73]
	K-means	[72]
	k-Nearest Neighbor	[74]
	Clustering	[75]

4.4. Intrusion detection

Intrusion detection is a process in which activities in a network or computer system are monitored for possible security problems. Intrusion detection involves monitoring of system activities, auditing of system vulnerabilities, statistical analysis of activity patterns, and abnormal activity analysis. Table 4 summarizes some of the quantitative intrusion detection methods. Intrusion detection methods fall into two categories: signature-based and anomaly-based detection [64].

Signature-based detection, also known as misuse detection, detects known attacks based on system behavior. Signature-based detection methods include state transition analysis and Petri nets. Ilgun et al. [65] introduced an approach to representing and detecting computer penetrations using a state transition diagram. This approach models penetrations as a series of state changes that lead from an initial secure state to a target compromised state. Vigna and Kemmerer [66] developed a network-based intrusion detection approach based on an extended state transition analysis technique (i.e., NetSTAT). NetSTAT was used to build a formal model of attack scenario using a state transition diagram. By using the formal model of the attack, NetSTAT is capable of determining which network events should be monitored. Ho et al. [67] proposed an intrusion detection approach by combining partial order planning and executable Petri Nets. This approach is capable of detecting attacks with a predetermined undesirable behavior or state change. Kumar and Spafford [68] developed a Petri nets-based method for misuse intrusion detection. Knowledge about attacks was represented as colored Petri nets. The Petri nets represent the transition of system states along paths that lead to intruded states.

Anomaly-based detection detects unknown attacks using statistical methods and artificial intelligence. Ourston et al. [69] introduced an approach using hidden Markov models to detect complex Internet attacks. This method is capable of addressing the multi-step attack problem. Experimental results have shown that this method is more effective than classical machine learning techniques such as decision trees and ANNs. Mukkamala et al. [71] developed an attack detection method using artificial neural networks (ANNs) and support vector machines (SVMs). ANNs and SVMs were used to build the classifiers using a list of features. Experimental results have demonstrated that ANNs and SVMs are capable of detecting anomalies and known intrusions. Pan et al. [70] developed a hybrid attack detection method by combining ANNs and decision tree algorithms. Experimental results have demonstrated that ANNs can detect DoS and Probing attacks more effectively than detecting unauthorized access from a remote machine and authorized access to local super user attacks. Zhang et al. [73] developed a random forests-based network intrusion detection method. This method was demonstrated on an in intrusion detection dataset. Experimental results have shown that the proposed method can achieve a high detection rate with a low false positive rate. Gaddam et al. [72] developed an approach to anomaly detection using cascading K-means clustering and ID3 decision tree learning algorithms. This method was used to analyze a network anomaly dataset. Experimental results have shown that detection accuracy is up to 96.24% at a false positive rate of 3%. Liao and Vemuri [74] developed a classifier for intrusion detection using the k-Nearest Neighbor (kNN) algorithm. This method was used to classify program behavior as normal or intrusive. Experimental results have shown that the kNN classifier can effectively detect intrusive attacks with a low false positive rate. Sabhnani and Serpen [76] analyzed an intrusion detection dataset using a set of machine learning algorithms. The dataset involves four types of major attacks, including probing, DoS, user-to-root, and remote-to-local attacks. Simulation results have demonstrated that certain classification algorithms are more effective for a given attack category. Lee et al. [75] introduced a cluster analysis-based attack detection method to detect DoS attacks proactively. A hierarchical clustering algorithm was used to analyze an intrusion detection data set. Experimental results have shown that this method is capable of detecting DoS attacks.

5. Risk determination

Risk determination involves assessing the level of risk to a manufacturing system. Mathematical modeling methods based on probability theory, fuzzy setts, neural networks are usually used to assess risk levels. Cherdantseva et al. [77] conducted a review of cybersecurity risk assessment methods for SCADA systems. An overview of twenty-four risk assessment methods for SCADA systems was provided. Table 5 lists some of the risk assessment methods.

Phillips and Swiler [78] developed an attack graph-based approach to computer network vulnerability analysis. A node represents a possible attack state. An edge represents a change of state caused by an action performed by an attacker. The attack graph is automatically generated given three types of inputs, including attack templates, a configuration file, and an attacker profile. The attack graph can be used to identify attack paths that are most likely to succeed or to simulate various attacks. Byres [79] developed an attack tree-based method for assessing security risks in the protocol specifications. Eleven possible attacker goals and security vulnerabilities in MODBUS-based SCADA systems were identified. The attack tree method was used to model system vulnerabilities. McQueen et al. [80] developed an approach to quantitative cyber risk reduction estimation for small SCADA control systems. The approach is based on a compromise graph where the nodes represent the stages of a potential attack and the edges represent the expected time-to-compromise. The time-to-compromise is modeled as a function of known vulnerabilities and attacker skill levels. Experimental results have shown that the compromise graph-based approach can increase the estimated time-to-compromise by about 3%–30%. Patel et al. [81] introduced an augmented vulnerability tree-based approach to measure the level of cybersecurity for SCADA systems. The threat-impact index and the cyber-vulnerability index were proposed to assess the vulnerabilities of SCADA systems. The approach was demonstrated on a SCADA testbed. Experimental results have shown that the approach is capable of quantifying the risks resulted from cyber threats effectively.

Table 5
A list of quantitative risk analysis methods.

Method	Reference
Attack graph	[78]
Attack tree	[79]
Compromise graph	[80]
Augmented vulnerability tree	[82]
Vulnerability tree	[81]
Petri nets	[83]
Process control network	[84]
Attack countermeasure tree	[85]
Digraph model	[86]
Anomaly-based intrusion detection	[87]
Boolean logic driven Markov process	[88]
Game theory	[89]

Henry et al. [83] developed an approach to quantify the risk of cyber-attacks on SCADA systems using Petri Nets. This approach enables a formal assessment of candidate policies to manage risks by the diminishing aspects of the network vulnerability to intrusion. A new algorithm was developed to automatically generate the Petri net model that represents a SCADA system. Experimental results have shown that the approach is capable of evaluating the security of a hazardous liquid loading process effectively. Roy et al. [85] introduced an attack-countermeasure tree-based method for modeling and analyzing cyber-attacks. The attack-countermeasure tree enables qualitative and probabilistic analysis of cyber-attacks as well as the optimization of defense strategies. Guan et al. [86] developed a digraph model that enables formal representation of SCADA systems. An algorithm was developed to perform the assessment of the impact of an at-risk component of a SCADA system. Experimental results have shown that the method can be used to identify the vulnerabilities of a SCADA system. Cardenas et al. [87] identified three challenges, including risk assessment, false-data-injection detection, and automatic attack-response, for securing process control systems. Detecting attacks to process control systems was formulated as an anomaly-based intrusion detection problem. By incorporating a physical model of a system, the most critical sensors and attacks can be identified. Several automatic response mechanisms were used for prevention, detection, and response to attacks. Kriaa et al. [88] introduced a method that can model the fundamental mechanisms of the Stuxnet attack using Boolean logic driven Markov processes. This method enables attack vectors and access points that an attacker may take control over the main control functions of a system. Hewett et al. [89] introduced an analytical game theoretic approach to analyzing the security of a SCADA system. A model of sequential, non-zero sum, two-player game between an attacker and a defender was constructed to mimic cyber-attacks on the SCADA system.

6. Conclusion

This paper provides a review of the most important aspects of cybersecurity in digital manufacturing with a particular focus on system characterization, identification of threats and vulnerabilities, attack scenarios, control methods, and risk determination techniques. As advanced sensing, high performance computing, artificial intelligence, and data analytics technologies are increasingly exploited in modern digital factories, cybersecurity is becoming a primary concern for manufacturers. Some of the biggest challenges facing both small- and medium-sized manufacturers and large original equipment manufacturers are identified as follows:

- The first challenge is that how manufacturers are able to secure legacy manufacturing machines and equipment that are increasingly retrofitted with remote monitoring, diagnosis, prognosis, control, and self-correction technologies. To address this challenge, new access control, encryption, intrusion detection techniques are required.
- The second challenge is that how manufacturers are able to detect and prevent embedded defects. Embedded defects refer to the defects introduced by attackers so that a system or a component will no longer perform its intended functions. To address this challenge, monitoring of manufacturing systems and processes as well as non-destructive testing (NDT) or non-destructive inspection (NDI) techniques are required.

Acknowledgements

The research reported in this paper was partially supported by the University of Central Florida and the Pennsylvania State University. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the University of Central Florida and the Pennsylvania State University. We thank Luoxia Cao from the University of Nevada, Reno who helped conduct the finite element simulation.

References

[1] Wu D, Liu S, Zhang L, Terpenny J, Gao RX, Kurfess T, et al. A fog computing-based framework for process monitoring and prognosis in cyber-manufacturing. J Manuf Syst 2017;43:25–34.
[2] Lu Y, Morris KC, Frechette S. Current standards landscape for smart manufacturing systems. National Institute of Standards and Technology, NISTIR; 2016. p. 8107.
[3] Davis J, Edgar T, Porter J, Bernaden J, Sarli M. Smart manufacturing, manufacturing intelligence and demand-dynamic performance. Comput Chem Eng 2012;47:145–56.
[4] Wu D, Rosen DW, Wang L, Schaefer D. Cloud-based design and manufacturing: a new paradigm in digital manufacturing and design innovation. Comput-Aided Des 2015;59:1–14.
[5] Wu D, Greer MJ, Rosen DW, Schaefer D. Cloud manufacturing: strategic vision and state-of-the-art. J Manuf Syst 2013;32(4):564–79.
[6] Wu D, Liu X, Hebert S, Gentzsch W, Terpenny J. Democratizing digital design and manufacturing using high performance cloud computing: performance evaluation and benchmarking. J Manuf Syst 2017;43:316–26.
[7] Xu X. From cloud computing to cloud manufacturing. Robot Comput-Integr Manuf 2012;28(1):75–86.
[8] Ren L, Zhang L, Tao F, Zhao C, Chai X, Zhao X. Cloud manufacturing: from concept to practice. Enterp Inf Syst 2015;9(2):186–209.
[9] Faruque A, Abdullah M, Chhetri SR, Canedo A, Wan J. Acoustic side-channel attacks on additive manufacturing systems. In: Proceedings of the 7th International Conference on Cyber-Physical Systems. 2016. p. 19.
[10] Sturm LD, Williams CB, Camelio JA, White J, Parker R. Cyber-physical vulnerabilities in additive manufacturing systems: a case study attack on the. STL file with human subjects. J Manuf Syst 2017;44:154–64.
[11] Turner H, White J, Camelio JA, Williams C, Amos B, Parker R. Bad parts: are our manufacturing systems at risk of silent cyberattacks? IEEE Secur Priv 2015;13(3):40–7.
[12] Kurfess T, Cass WJ. Rethinking additive manufacturing and intellectual property protection. Res-Technol Manag 2014;57(5):35–42.
[13] Vincent H, Wells L, Tarazaga P, Camelio J. Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. Procedia Manuf 2015;1:77–85.
[14] DeSmit Z, Elhabashy AE, Wells LJ, Camelio JA. Cyber-physical vulnerability assessment in manufacturing systems. Procedia Manuf 2016;5: 1060–74.
[15] Thames L, Schaefer D. Cybersecurity for industry 4.0. Springer; 2017.
[16] Zeltmann SE, Gupta N, Tsoutsos NG, Maniatakos M, Rajendran J, Karri R. Manufacturing and security challenges in 3D printing. JOM 2016;68(7):1872–81.
[17] Davis J. Cybersecurity for manufacturers: securing the digitized and connected factory; 2017.
[18] Wells LJ, Camelio JA, Williams CB, White J. Cyber-physical security challenges in manufacturing systems. Manuf Lett 2014;2(2):74–7.
[19] Maurushat A. Disclosure of security vulnerabilities: legal and ethical issues. Springer; 2013.
[20] NBCNews. <https://www.nbcnews.com/tech/security/cybercrime-costs-businesses-445-billion-thousands-jobs-study-n124746/>; 2014.
[21] Langner R. Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur Priv 2011;9(3):49–51.
[22] Igure VM, Laughter SA, Williams RD. Security issues in SCADA networks. Comput Secur 2006;25(7):498–506.
[23] Nicholson A, Webber S, Dyer S, Patel T, Janicke H. SCADA security in the light of Cyber-Warfare. Comput Secur 2012;31(4):418–36.
[24] Security, F. O. f. I. <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile%20/>; 2014.
[25] ABBGroup. <http://www.abb.com/cawp/seitp202/5a998d449645ac48c125810b0033b659.aspx/>; 2017.
[26] Science, N. C. f. M. <http://www.nam.org/Issues/Technology/Cybersecurity-in-the-Manufacturing-Sector//>; 2017.
[27] Stouffer K, Zimmerman T, Tang C, Lubell J, Cichonski J, McCarthy J. Cybersecurity framework manufacturing profile; 2017.
[28] Stoneburner G, Goguen AY, Feringa A. Sp 800-30. Risk management guide for information technology systems; 2002.
[29] Mulazzani M, Schrittwieser S, Leithner M, Huber M, Weippl ER. Dark Clouds on the Horizon: using Cloud Storage as Attack Vector and Online Slack Space. In: Proc. USENIX Security Symposium. 2011. p. 65–76.
[30] ATmega1284P datasheet summary, <http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-42719-ATmega1284P_Datasheet_Summary.pdf/>; 2018.
[31] Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based access control. ACM Trans Inf Syst Secur (TISSEC) 2001;4(3):224–74.
[32] Sandhu R, Ferraiolo D, Kuhn R. The NIST model for role-based access control: towards a unified standard. Proc. ACM Workshop on Role-Based Access Control 2000:1–11.
[33] Osborn S, Sandhu R, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies. ACM Trans Inf Syst Secur (TISSEC) 2000;3(2):85–106.
[34] Hu VC, Kuhn DR, Ferraiolo DF. Attribute-based access control. Computer 2015;48(2):85–8.
[35] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. In: Proc. Proceedings of the 13th ACM Conference on Computer and Communications Security. 2006. p. 89–98.
[36] Wang G, Liu Q, Wu J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. 2010. p. 735–7.
[37] Wang L, Wijesekera D, Jajodia S. A logic-based framework for attribute based access control. In: Proceedings of the 2004 ACM Workshop on Formal Methods in Security Engineering. 2004. p. 45–55.
[38] Corrad A, Montanari R, Tibaldi D. Context-based access control management in ubiquitous environments. In: Network Computing and Applications, 2004.(NCA 2004). Proceedings. Third IEEE International Symposium on. 2004. p. 253–60.
[39] Bhatti R, Bertino E, Ghafoor A. A trust-based context-aware access control model for web-services. Distrib Parallel Databases 2005;18(1):83–105.
[40] Shebaro B, Oluwatimi O, Bertino E. Context-based access control systems for mobile devices. IEEE Trans Dependable Secure Comput 2015;12(2):150–63.
[41] McCloghrie K, Wijnen B, Presuhn R. View-based access control model (VACM) for the simple network management protocol (SNMP); 2002.
[42] Gabillon A, Letouzey L. A view based access control model for SPARQL. In: Network and System Security (NSS), 2010 4th International Conference on. 2010. p. 105–12.
[43] Finin T, Joshi A, Kagal L, Niu J, Sandhu R, Winsborough W, Thuraisingham B. R OWL BAC: representing role based access control in OWL. In: Proceedings of the 13th ACM Symposium on Access Control Models and Technologies. 2008. p. 73–82.
[44] Ferrini R, Bertino E. Supporting rbac with xacml+ owl. In: Proceedings of the 14th ACM Symposium on Access Control Models and Technologies. 2009. p. 145–54.

Please cite this article in press as: Wu D, et al. Cybersecurity for digital manufacturing. J Manuf Syst (2018), https://doi.org/10.1016/j.jmsy.2018.03.006

[45] Priebe T, Dobmeier W, Kamprath N. Supporting attribute-based access control with ontologies. In: Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on. 2006. p. 8–472.
[46] Cirio L, Cruz IF, Tamassia R. A role and attribute based access control system using semantic web technologies. In: OTM Confederated International Conferences On the Move to Meaningful Internet Systems. 2007. p. 1256–66.
[47] Corradi A, Montanari R, Tibaldi D. Context-based access control for ubiquitous service provisioning. Proc. Computer Software and Applications Conference, COMPSAC 2004. Proceedings of the 28th Annual International, IEEE 2004:444–51.
[48] Montanari R, Toninelli A, Bradshaw JM. Context-based security management for multi-agent systems. Proc. Multi-Agent Security and Survivability, IEEE 2nd Symposium on, IEEE 2005:75–84.
[49] Barker WC, Barker EB. SP 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm (TDEA) block cipher; 2012.
[50] Coppersmith D. The data encryption standard (DES) and its strength against attacks. IBM J Res Dev 1994;38(3):243–50.
[51] Miller FP, Vandome AF, McBrewster J. Advanced encryption standard; 2009.
[52] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 1978;21(2):120–6.
[53] Schneier B. Description of a new variable-length key, 64-bit block cipher (Blowfish). In: Proc. International Workshop on Fast Software Encryption. 1993. p. 191–204.
[54] Schneier B, Kelsey J, Whiting D, Wagner D, Hall C, Ferguson N. Twofish: a 128-bit block cipher, NIST AES proposal; 1998. p. 15.
[55] Brostoff S, Sasse MA. Are Passfaces more usable than passwords? A field trial investigation. In: People and computers XIV—usability or else!. Springer; 2000. p. 405–24.
[56] Perrig A, Dhamija R. Déja vu: A user study using images for authentication. Proc. USENIX Security Symposium 2000.
[57] Jermyn I, Mayer A, Monrose F, Reiter MK, Rubin AD. The design and analysis of graphical passwords. USENIX Association; 1999.
[58] Monrose F, Rubin A. Authentication via keystroke dynamics. In: Proc. Proceedings of the 4th ACM Conference on Computer and Communications Security. 1997. p. 48–56.
[59] Giuffrida C, Majdanik K, Conti M, Bos H. I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. In: Proc. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. 2014. p. 92–111.
[60] Zheng N, Paloski A, Wang H. An efficient user verification system via mouse movements. In: Proc. Proceedings of the 18th ACM Conference on Computer and Communications Security. 2011. p. 139–50.
[61] Xu K, Xiong H, Wu C, Stefan D, Yao D. Data-provenance verification for secure hosts. IEEE Trans Dependable Secure Comput 2012;9(2):173–83.
[62] Kholmatov A, Yanikoglu B. Identity authentication using improved online signature verification method. Pattern Recognit Lett 2005;26(15):2400–8.
[63] Muda AK, Choo Y-H, Abraham A, Srihari SN. Computational intelligence in digital forensics: forensic investigation and applications. Springer; 2014.
[64] Kaur P, Kumar M, Bhandari A. A review of detection approaches for distributed denial of service attacks. Syst Sci Control Eng 2017;5(1):301–20.
[65] Ilgun K, Kemmerer RA, Porras PA. State transition analysis: a rule-based intrusion detection approach. IEEE Trans Softw Eng 1995;21(3):181–99.
[66] Vigna G, Kemmerer RA. NetSTAT: A network-based intrusion detection approach. Proc. Computer Security Applications Conference, 1998. Proceedings. 14th Annual, IEEE 1998:25–34.
[67] Ho Y, Frincke D, Tobin D. Planning, petri nets, and intrusion detection. Proc. Proceedings of the 21st National Information Systems Security Conference 1998:346–61.
[68] Kumar S, Spafford EH. A pattern matching model for misuse intrusion detection; 1994.
[69] Ourston D, Matzner S, Stump W, Hopkins B. Applications of hidden markov models to detecting multi-stage network attacks. In: Proc. System Sciences, Proceedings of the 36th Annual Hawaii International Conference on. 2003. p. 10.
[70] Pan Z-S, Chen S-C, Hu G-B, Zhang D-Q. Hybrid neural network and C4. 5 for misuse detection. In: Proc. Machine Learning and Cybernetics, 2003 International Conference on. 2003. p. 2463–7.
[71] Mukkamala S, Janoski G, Sung A. Intrusion detection using neural networks and support vector machines. Proc. Neural Networks, IJCNN'02. Proceedings of the 2002 International Joint Conference on, IEEE 2002:1702–7.
[72] Gaddam SR, Phoha VV, Balagani KS. K-Means+ ID3: a novel method for supervised anomaly detection by cascading K-Means clustering and ID3 decision tree learning methods. IEEE Trans Knowl Data Eng 2007;19(3):345–54.
[73] Zhang J, Zulkernine M, Haque A. Random-forests-based network intrusion detection systems. IEEE Trans Syst Man Cybern Part C (Appl Rev) 2008;38(5):649–59.
[74] Liao Y, Vemuri VR. Use of k-nearest neighbor classifier for intrusion detection. Comput Secur 2002;21(5):439–48.
[75] Lee K, Kim J, Kwon KH, Han Y, Kim S. DDoS attack detection method using cluster analysis. Expert Syst Appl 2008;34(3):1659–65.
[76] Sabhnani M, Serpen G. Application of machine learning algorithms to KDD intrusion detection dataset within misuse detection context. Proc. MLMTA 2003:209–15.
[77] Cherdantseva Y, Burnap P, Blyth A, Eden P, Jones K, Soulsby H, et al. A review of cyber security risk assessment methods for SCADA systems. Comput Secur 2016;56:1–27.
[78] Phillips C, Swiler LP. A graph-based system for network-vulnerability analysis. In: Proc. Proceedings of the 1998 Workshop on New Security Paradigms. 1999. p. 71–9.
[79] Byres EJ, Franz M, Miller D. The use of attack trees in assessing vulnerabilities in SCADA systems. Proc. Proceedings of the International Infrastructure Survivability Workshop 2017.
[80] McQueen MA, Boyer WF, Flynn MA, Beitel GA. Quantitative cyber risk reduction estimation methodology for a small SCADA control system. In: Proc. System Sciences, HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on. 2006. p. 226.
[81] Patel SC, Graham JH, Ralston PA. Quantitatively assessing the vulnerability of critical information systems: a new method for evaluating security enhancements. Int J Inf Manag 2008;28(6):483–91.
[82] Ralston PA, Graham JH, Hieb JL. Cyber security risk assessment for SCADA and DCS networks. ISA Trans 2007;46(4):583–94.
[83] Henry MH, Layer RM, Snow KZ, Zaret DR. Evaluating the risk of cyber attacks on SCADA systems via Petri net analysis with application to hazardous liquid loading operations. In: Proc. Technologies for Homeland Security, HST'09. IEEE Conference on. 2009. p. 607–14.
[84] Henry MH, Haimes YY. A comprehensive network security risk model for process control networks. Risk Anal 2009;29(2):223–48.
[85] Roy A, Kim DS, Trivedi KS. Cyber security analysis using attack countermeasure trees. In: Proc. Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. 2010. p. 28.
[86] Guan J, Graham JH, Hieb JL. A digraph model for risk identification and mangement in SCADA systems. In: Proc. Intelligence and Security Informatics (ISI), 2011 IEEE International Conference on. 2011. p. 150–5.
[87] Cárdenas AA, Amin S, Lin Z-S, Huang Y-L, Huang C-Y, Sastry S. Attacks against process control systems: risk assessment, detection, and response. In: Proc. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. 2011. p. 355–66.
[88] Kriaa S, Bouissou M, Piètre-Cambacédès L. Modeling the Stuxnet attack with BDMP: towards more formal risk assessments. In: Proc. Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference on. 2012. p. 1–8.
[89] Hewett R, Rudrapattana S, Kijsanayothin P. Cyber-security analysis of smart grid SCADA systems with game models. In: Proc. Proceedings of the 9th Annual Cyber and Information Security Research Conference. 2014. p. 109–12.

Please cite this article in press as: Wu D, et al. Cybersecurity for digital manufacturing. J Manuf Syst (2018), https://doi.org/10.1016/j.jmsy.2018.03.006