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.



## 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/

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.

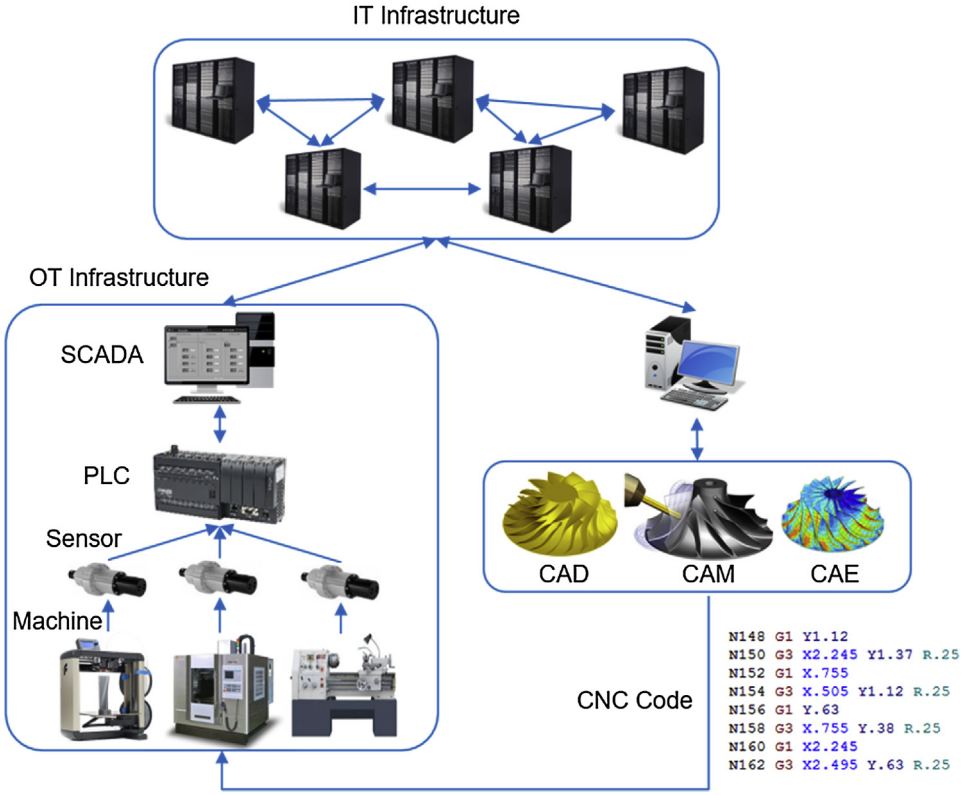


**Fig. 1.** Manufacturing system model.

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