Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 00 (2019) 000–000

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

29th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM2019), June 24-28, 2019, Limerick, Ireland.

Cybersecurity Concerns for Total Productive Maintenance in Smart Manufacturing Systems

Alireza Zarreh[a], HungDa Wan[a*], Yooneun Lee[a], Can Saygin[a], Rafid Al Janahi[a]

[a] *Department of Mechanical Engineering and Center for Advanced Manufacturing and Lean Systems, University of Texas at San Antonio, San Antonio, Texas, USA*

Abstract

Maintenance is the core function to keep a system running and avoid failure. Total Productive Maintenance (TPM) has broadly utilized maintenance strategy to improve the customer's satisfaction and hence obtain a competitive advancement. However, the complexity of smart manufacturing systems due to the recent advancements, specifically the integration of internet and network systems with traditional manufacturing platforms, has made this function more challenging. The focus of this paper is to explain how cybersecurity could impact the TPM by affecting the overall equipment effectiveness (OEE) in a smart manufacturing system by providing a structured literature survey. First, it provides concerns on principle of TPM regarding cybersecurity in smart manufacturing systems. Then, it highlights the effect of a variety of cyber-physical threats on OEE, as a main key performance indicator of TPM and how differently they can reduce OEE. The countermeasures that could be considered to compensate for the negative impact of a cybersecurity threat on the overall effectiveness of the system also will be discussed. Finally, research gaps and challenges are identified to improve overall equipment effectiveness (OEE) in presence of cybersecurity threats in critical manufacturing industries.

Keywords: Cyber security in Manufacturing; Total Productive Maintenance; Smart manufacturing systems; Overall Equipment Effectiveness;

1. Introduction

The increasing trend of adoption of smart features in manufacturing systems has helped improve productivity and quality as well as profit by revolutionizing the whole manufacturing paradigm (Figure 1). However, interconnectivity at production level makes them vulnerable to cyber threats [1]. Even though most of these threats are not new to IT world, there are new concerns in manufacturing systems regarding cybersecurity. Though most of the research has been done in the field of threats to intellectual properties (IPs) including stealing and modifying them, this is not the only concern of smart manufacturing systems.

Due to increasing utilization of cyber-physical systems, autonomous robots, and internet of things (IoT), any cyber-physical threat not only harms the integrity of the IPs but also can potentially disrupt production process and even bring a hazardous situation to the system [2].

To reduce disruption and increase productivity, one of the pillars of implementing lean concept is total productive maintenance (TPM). The goals of TPM are zero breakdown, no slow running, no defects, and making the production environment safe and in a perfect condition [3]. However, the cybersecurity threats could directly disrupt these goals by provoking system failure, slow running and quality problems [4,5].

This paper intends to demonstrate the effects of cybersecurity threats on leanness of the system by discussing the impact of cyber-physical threats on principles of TPM and overall equipment effectiveness (OEE) as its key performance indicator (KPI). A structured review of previous research provides evidence of the proposed concepts. While other researchers mostly attempted to demonstrate the effect of cybersecurity threats in terms of monetary consequences [6,7], this paper emphasizes on their effects on leanness of the system and its performance.

The remaining contents are organized as follows. Section 2 elaborates and discusses new challenges brought by recent integration of the cyber world with the traditional manufacturing world on the main principles of the total productive maintenance. Section 3 explains the effects of these threats on each of the components of the OEE of the system as the main KPI of TPM. Section 4 discusses further concerns of cybersecurity in a lean smart manufacturing and concludes the paper with suggestions for the future works.

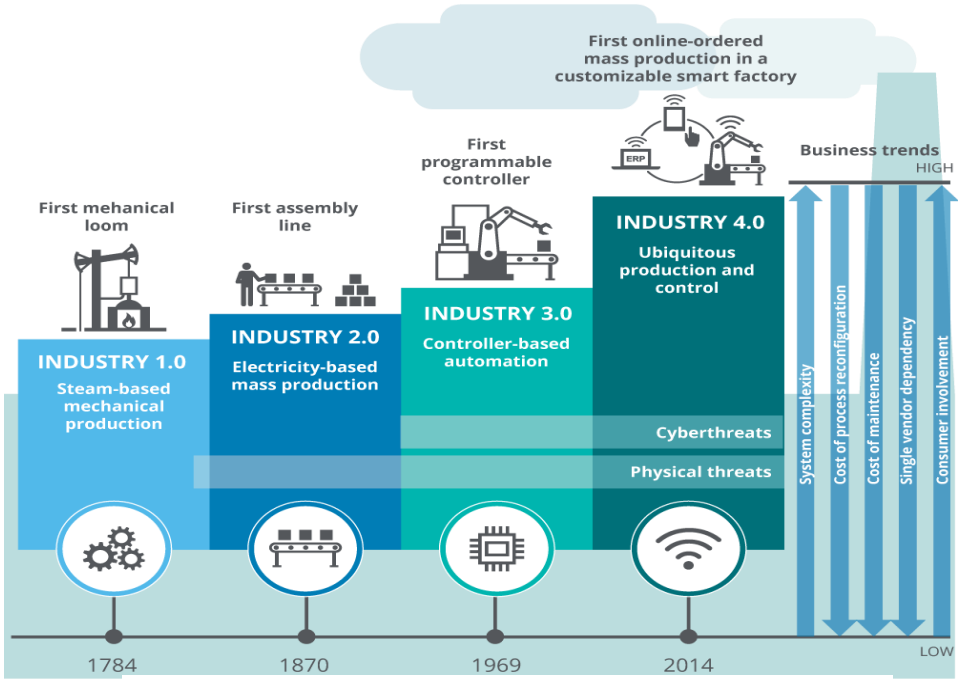

Figure 1. Progression of cyber and physical threats for each industrial revolution [1]

2. Cybersecurity versus the pillars of TPM

The traditional TPM model consists of eight principles, also referred as the pillars of the TPM, namely, autonomous maintenance, focused improvement, planned maintenance, quality management, development management, education and training, administrative & office TPM, and safety health environment [8]. The base of these pillars is that 5S method that tries to make a well-organized work environment by five actions: sort, set in order, shine, standardize, and sustain [9]. In this section, the eight pillars are discussed with respect to threats and concerns of cybersecurity toward each of them.

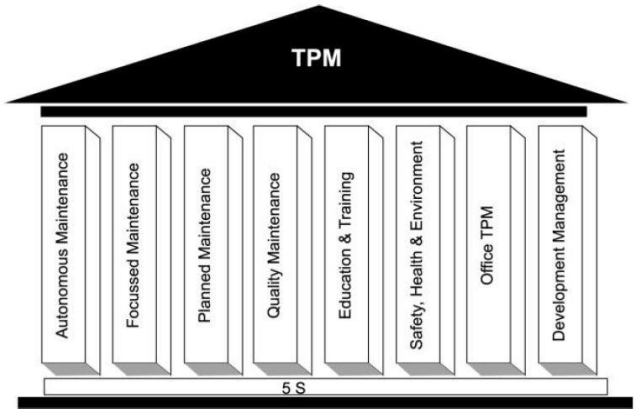

Figure 2. The traditional TPM model consists of a 5S foundation (Sort, Set in Order, Shine, Standardize, and Sustain) and eight supporting activities [8]

2.1. Autonomous maintenance

This pillar is the mother pillar of TPM. It places routine maintenances of machines such as cleaning, lubrication, inspection, and adjusting in the operator's hand. It brings the ownership attitude to the operator of the machine. This way the maintenance personnel will be freed to perform a higher-level task.

According to literatures [10,11] the system is subject to vulnerabilities whenever a human entity is interacting with cyber entities. Introducing new and complicated machines to do tasks such as inspection could be very challenging to operators. Since operators are normally less computer savvy, it will be hard for them to recognize cyber threats and possible alterations in their jobs that could be coming from cybersecurity breach. Wells et al. [12] illustrate the weakness of the operators' knowledge by a case study in which they altered the transferred file for a CNC machine by a virus and result was that only a few groups determined the quality issue in the product and none could diagnose the source of the problem.

2.2. Focused improvement

This pillar aims to improve overall equipment effectiveness (OEE) by minimizing waste in the system. Normally it is deployed by a small group of employees that regularly identify and resolve recurring problems in order to incrementally improve the operation of the equipment.

Based on the Bekar et al. [13] research in industry 4.0 cybersecurity concerns is a pressing issue for this pillar. They reached to this conclusion by collecting opinions of the decision makers including TPM, Production, and Quality managers to measure the impact of key technologies of Industry 4.0.

2.3. Planned Maintenance

Planned maintenance is prescheduled repairs, adjustments or replacing of a part due to an inspection that increases the life span of the machine and prevents breakdown. The schedule is normally created according to historical or predicted failure rates.

The cybersecurity concern for this pillar is to have a proper prescheduled preventive maintenance not only for traditional machines but also to have it for the network, mobile devices, and RFIDs, hardware and software as well [14–16]. These planned maintenances are the main way to prevent or mitigate the impact of a cyber-attack.

2.4. Quality maintenance

Quality maintenance aims to have a zero defect in products and processes through analysis of root causes of failures and defects to eliminate the source of the quality defects. In the new age of manufacturing, there are two challenges regarding the quality of the product. The first challenge is to detect the quality issue in a product and the second one is to find the source of the failure and eliminate it. This argument will be further discussed in the OEE section.

2.5. Education and Training

Education and training are one of the most essential principles of TPM that ensures that the employees and staff involved with the TPM have the proper knowledge and skills to have a successful deployment of TPM. This principle must get more serious attention since manufacturing systems often lack qualified employees regarding the skill and knowledge for cybersecurity incorporation with the production system [17,18]. Training current and future TPM employees including operators, maintenance staff, and managers on the potential threats of cybersecurity plays a key role in having a successful TPM implementation for smart manufacturing systems [19].

2.6. Safety Health Environment

This principle tends to implement a methodology to maintain a safe and healthy environment for all staff and employees by eliminating potential health and safety risks to reach an accident-free workplace. This principle is also exposed to vulnerabilities from cybersecurity threat. According to Wu et al. [20] in a cyber manufacturing system human can be targeted as the victim. Operators, assembly workers working close to autonomous robots and machines are endangered when hackers can send malicious control to actuators [21].

Moreover, by increasing the trend of using safety-critical mechanical systems such as next-generation composite aircraft, sustainable energy, artificial heart valves, automated drug dispensary equipment, high-speed rail systems, and gas turbines any interruption or alteration in their precise engineering could cause a significant safety problem [22–25].

2.7. Office TPM

Office TPM is to provide all necessary administrative support in all areas of the system and apply TPM techniques to administrative functions. It extends the benefits of TPM beyond the floor plans. Some losses addressed by office TPM are processing and communication losses, office equipment breakdown, and communication channel breakdown [26,27]. This is the area in which the traditional IT cybersecurity is involved. In this part, the main threats to the system are compromising and stealing of intellectual properties of a company.

2.8. Early/equipment management

Early equipment management or also called development management tends to minimize the problems and running time for installing new equipment. Also, it improves the development of the new equipment by directing practical knowledge and understanding gained from TPM [28]. Clearly, for smart manufacturing system considering cybersecurity issues for the development of new equipment with the minimal problem is important.

Table 1 is summarizing the cybersecurity concerns in manufacturing systems regarding each pillar of TPM. It also provides related literature for each pillar. As can be seen from in this table while some of the pillars have received more attention from the research community others such as focused improvement and development management pillars demonstrate opportunities for researches.

Table 1. eight pillars of TPM and their cybersecurity concerns

TPM Principle	Cybersecurity concerns	Related literature
Autonomous Maintenance	Less computer savvy operators	[10–12,18]
Focused improvement	Consideration of losses regarding cyber-physical security	[13]
Planned maintenance	Planning effective PM to prevent and mitigate cyber-physical attacks	[14–16]
Quality maintenance	Detecting a quality issue regarding cyber-physical attacks and the ability to analyze its source	[29–31]
Education and training	Improving cybersecurity skills and awareness of operators, maintenance staff, and management	[17–19]
Safety, health, and environment	Eliminate incidents of injuries and accidents caused by cyber threats	[20–25]
Office TPM	Addressing traditional IT cybersecurity, securing intellectual properties, data and network	[13,26,27]
Development management	Minimal cybersecurity problems from new equipment	[28]

3. Overall Equipment Effectiveness

Overall equipment effectiveness (OEE) is the main KPI to measure the effectiveness of TPM in a system. It identifies the percentage of planned production time that is truly productive. Equation 1 demonstrates the model to calculate OEE of a system. It consists of three components that are aligned with the TPM goals of no breakdowns (measured by availability), no small stops or slow running (measured by performance), and no defects (measured by quality) and each component contribute with a type of productivity loss. Each of these components can be affected by the cyber-physical attack that is discussed in the following sub-sections.

$$OEE = Availability \times Performance \times Quality \tag{1}$$

3.1. Availability

Availability takes into account losses that cause a stop in planned production for a considerable length of time (typically several minutes or longer). It includes breakdowns, repairs, changeover, adjustment and startups. As a common result of cyber-attacks, the availability of the system could be lost.

Industrial control systems could be a primary target for attackers in a manufacturing system. Due to the complexity of industrial control, system attackers need to have high skills and familiarity with the control system to execute an attack. As a result, these attacks normally are a state or a government funded. Li et al. [32] demonstrate that many physical processes controlled by SCADA system could be targeted in a cyber-physical system.

The most famous attack to this day has been a worm called Stuxnet that attacked the Iranian nuclear enrichment plant in Natanz in 2009 and 2010. It does little or no harm to computers, instead, it checks if the computer is connected to programmable logic controllers (PLCs). If so, it alters the PLCs' programming, results to centrifuges spun too fast for too long which causes the destruction of the equipment [33,34]. Another incident is the infection of the industrial control system of German Steel Mill that caused failure in multiple components of the system [35].

However, the threat to availability is not just the infection of control systems. Availability loss could be the result of a different mechanism. For instance, infection of computers in manufacturing plant with WannaCry virus caused Honda, the automobile manufacturer, to shut down production in a plant. This virus takes advantage of legacy systems and takes control of the infected computer and demands payment via Bitcoin [36].

3.2. Performance

Performance considers losses that happened because of the performance of the production system with less than the maximum possible running speed. It includes slow cycles and short stoppages. In the case of a cybersecurity attack, there are many scenarios that could lead to longer cycle time and hence decrease the performance of the system.

One of these scenarios is to change the process parameters of the system which leads the system to perform with lower yield rate. This applies to both additive manufacturing and subtractive manufacturing. In subtractive manufacturing simply changing the G-code or M-code to make the spindle or the feed rate work slower not only will cause a longer production but also could potentially change the mechanical properties of the product [37,38]. This could be worsen when metals and alloys are used and could endanger the system where weak or damaged components are used in safety-critical systems, potentially endanger human lives [39,40]. Similarly, any alteration in nozzle speed or motion of printer head in additive manufacturing could result in lower performance [41–43].

Information delay has an adverse effect on flexible manufacturing system performance rate and the potential to disrupt production schedules [44]. Also, with the increasing demand for utilizing cloud manufacturing any interruption with the resource allocation, service composition and service operation management could adversely affect system performance [45–47]. An attack can drastically reduce performance by altering a manufacturing system, resulting in impaired communication, functionality or reduced performance [48].

One of the most significant vulnerabilities of manufacturing systems regarding performance is probably supply chain security. With the highly outsourced supply chain and dependability on suppliers for manufacturing systems, any interruption in the supply chain could cause a delay of satisfying customer demands. In a recent incident, a virus attack to a supplier of Apple Co. delayed the shipment of the company's products. The Taiwan Semiconductor Manufacturing Company – the world's largest chip manufacturer – was forced to shut down production for a few days. The company said some of the computers and 80% of its manufacturing tools had been infected by a virus [49].

3.3. Quality

Quality takes into account losses when a manufactured part or product do not meet quality standards. It includes product rejects, scraps and reworks. Wells et al. [12] mention quality control as one of the weaknesses in manufacturing systems regarding the cybersecurity. The first issue can come from the silent cyber-attacks when the system cannot catch the quality changes made by a malicious attack. It could happen when the quality control process is under attack as well as the production system [22]. In these circumstances, there are two ways that an attack could harm the system. Firstly, by making the system accept bad parts that even though it will not affect OEE directly will cause problems later and secondly, by rejecting good quality parts by inserting faulty criteria. Zeltmann et al. [29] describe a situation in which the quality of a part is compromised in additive manufacturing by alteration in printing direction which would pass the quality control completely undetected.

Table 2. Cybersecurity incident example for OEE components

OEE Component	Incident example	Reference	Year	Consequence of attack
Availability				
	German Mill	[35]	2008	Machine Breakage, Risk of injuries
	Honda's car manufacturer	[36]	2008	system shutdown
	Iranian Nuclear Enrichment Plant	[34]	2010	Failure of 20% of plant
	Chrysler's car manufacturing plants	[50]	2005	13 plants went offline
Performance				
	Taiwan Semiconductor Manufacturing Company (TSMC)	[49]	2018	Availability of Apple's new iPhones
	Target supply chain	[51]	2013	Customers' data was stolen
Quality				
	CMS malicious void attack	[20]	2017	Defective parts
	water purification company	[50]	2002	Dad quality water

Considering having the integrity of the quality control process intact, a variety of attack methods could directly affect the quality of a product [30]. This could be done through altering part quality definitions, reporting falsified data, acquiring QC implementation data, altering product design and altering manufacturing processes. Sturm et al [31] describe also the vulnerability of using .STL files in additive manufacturing that could cause quality issues.

Table 2 presents a few examples of cybersecurity incidents for each of OEE components. This should be mentioned that sometimes one incident could cause harm to more than one component of OEE. For example, any interruption in the availability of a company which is the supplier of a bigger one could harm the performance of the bigger company.

4. Discussion and conclusion

The best way to defend a system and mitigate cybersecurity threat in a system is actually having a reliable TPM that could ensure and protect them from these threats. To implement such a TPM in a system, it is necessary to consider all factors involved with the interconnectivity of cyber and physical domain in a smart manufacturing system. These factors could jeopardize the availability, performance, and quality of the system as well as safety concerns which are the primary goals of TPM.

Some of these threats could instantly harm the system by reducing availability, performance or quality of the system. However, there are threats that target the integrity of the system which it will have an indirect effect on the productivity of the system; which sometimes does not affect it instantly. Another concern regarding the cybersecurity of a lean system with implemented TPM is the visibility of a cyber-attack. As the number of attacks has been increasing over the past decade the visibility of these attacks is decreased that means it is getting harder to discover a cyber-attack in a system [12]. So designing a proper defense policy and quality assurance system to discover all interference in the system is essential. Moreover, have a low recovery time, also considered as repair time, is very important to have an agile maintenance system. Mean time between failure (MTBF) and mean time to repair (MTTR) as the contributor factors to the availability of a system depends directly on low repair time. So, having a proper plan for recovery from an attack and to do all the repairs in minimum time plays an important role in the availability of the system.

For future works, evaluating and assessing cybersecurity in manufacturing systems considering their unique characteristics which differentiate it from the traditional IT security is necessary. Measuring the consequence of attacks in term of overall equipment effectiveness and not in monetary format could provide a new insight into this domain. Lastly, as it was shown in this paper some of the pillars of TPM has not received enough attention regarding cybersecurity issues which could be considered for future research direction. Similarly, regarding OEE most of the researches focus on the effect of cybersecurity concerns on availability and quality which leave the performance as another future research opportunity.

References

[1] Cyber risk in advanced manufacturing | Deloitte US, Deloitte U. S. (2017).
[2] N. Tuptuk, S. Hailes, Security of smart manufacturing systems, J. Manuf. Syst. 47 (2018) 93–106.
[3] O.T.R. Almeanazel, Total productive maintenance review and overall equipment effectiveness measurement, Jordan J. Mech. Ind. Eng. 4 (2010).
[4] A. Bracho, C. Saygin, H. Wan, Y. Lee, A. Zarreh, A simulation-based platform for assessing the impact of cyber-threats on smart manufacturing systems, Procedia Manuf. 26 (2018) 1116–1127.
[5] A.J.B. Avila, Assessing the Impact of Cyber-Threats on Smart Manufacturing Systems through a Simulation Study, PhD Thesis, The University of Texas at San Antonio, 2017.
[6] A. Zarreh, C. Saygin, H. Wan, Y. Lee, A. Bracho, Cybersecurity Analysis of Smart Manufacturing System Using Game Theory Approach and Quantal Response Equilibrium, Procedia Manuf. 17 (2018) 1001–1008.
[7] A. Zarreh, C. Saygin, H. Wan, Y. Lee, A. Bracho, A game theory based cybersecurity assessment model for advanced manufacturing systems, Procedia Manuf. 26 (2018) 1255–1264.
[8] J. s. Khamba, I. p. s. Ahuja, Total productive maintenance: literature review and directions, Int. J. Qual. Reliab. Manag. 25 (2008) 709–756.
[9] M. Moradi, M.R. Abdollahzadeh, A. Vakili, Effects of implementing 5S on Total Productive Maintenance: A case in Iran, in: 2011 IEEE Int. Conf. Qual. Reliab., 2011: pp. 41–45.
[10] Z. DeSmit, A.E. Elhabashy, L.J. Wells, J.A. Camelio, An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems, J. Manuf. Syst. 43 (2017) 339–351.
[11] Z. DeSmit, A.E. Elhabashy, L.J. Wells, J.A. Camelio, Cyber-physical vulnerability assessment in manufacturing systems, Procedia Manuf. 5 (2016) 1060–1074.
[12] L.J. Wells, J.A. Camelio, C.B. Williams, J. White, Cyber-physical security challenges in manufacturing systems, Manuf. Lett. 2 (2014) 74–77.
[13] E.T. Bekar, A. Skoogh, N. Cetin, O. Siray, Prediction of Industry 4.0's Impact on Total Productive Maintenance Using a Real Manufacturing

Case, in: Int. Symp. Prod. Res., Springer, 2018: pp. 136–149.
[14] K.S. Trivedi, D.S. Kim, A. Roy, D. Medhi, Dependability and security models, in: 2009 7th Int. Workshop Des. Reliab. Commun. Netw., 2009: pp. 11–20.
[15] F. Sahba, A. Sahba, R. Sahba, Helping Blind People in Their Meeting Locations to Find Each Other Using RFID Technology, Int. J. Comput. Sci. Inf. Secur. 16 (2018) 123–127.
[16] Y. Guo, C. Ten, S. Hu, W.W. Weaver, Preventive Maintenance for Advanced Metering Infrastructure Against Malware Propagation, IEEE Trans. Smart Grid. 7 (2016) 1314–1328.
[17] A. Benešová, J. Tupa, Requirements for Education and Qualification of People in Industry 4.0, Procedia Manuf. 11 (2017) 2195–2202.
[18] U.D. Ani, H. He, A. Tiwari, Human factor security: evaluating the cybersecurity capacity of the industrial workforce, J. Syst. Inf. Technol. (2018).
[19] S.M.L. Coalition, Implementing 21st century smart manufacturing, in: Workshop Summ. Rep., 2011.
[20] M. Wu, Y.B. Moon, Taxonomy of cross-domain attacks on cybermanufacturing system, Procedia Comput. Sci. 114 (2017) 367–374.
[21] P. Shahmaleki, M. Mahzoon, Designing a hierarchical fuzzy controller for backing-up a four wheel autonomous robot, in: 2008 Am. Control Conf., IEEE, 2008: pp. 4893–4897.
[22] H. Turner, J. White, J.A. Camelio, C. Williams, B. Amos, R. Parker, Bad parts: Are our manufacturing systems at risk of silent cyberattacks?, IEEE Secur. Priv. 13 (2015) 40–47.
[23] F. Sahba, R. Sahba, Prevention of Metro Rail Accidents and Incidents in Stations Using RFID Technology, in: 2018 World Autom. Congr. WAC, IEEE, 2018: pp. 1–5.
[24] M. Bagheri, M. Madani, R. Sahba, A. Sahba, Real time object detection using a novel adaptive color thresholding method, in: Proc. 2011 Int. ACM Workshop Ubiquitous Meta User Interfaces, ACM, 2011: pp. 13–16.
[25] P. Shahmaleki, M. Mahzoon, GA modeling and ANFIS control design for a solar power plant, in: Proc. 2010 Am. Control Conf., IEEE, 2010: pp. 3530–3535.
[26] D. Glavach, J. LaSalle-DeSantis, S. Zimmerman, Applying and assessing cybersecurity controls for direct digital manufacturing (ddm) systems, in: Cybersecurity Ind. 40, Springer, 2017: pp. 173–194.
[27] L.B.A. Rabai, M. Jouini, A.B. Aissa, A. Mili, A cybersecurity model in cloud computing environments, J. King Saud Univ.-Comput. Inf. Sci. 25 (2013) 63–75.
[28] J. Alander, Applying lean principles to order-to-delivery process for spare parts with embedded software, (2016).
[29] S.E. Zeltmann, N. Gupta, N.G. Tsoutsos, M. Maniatakos, J. Rajendran, R. Karri, Manufacturing and security challenges in 3D printing, Jom. 68 (2016) 1872–1881.
[30] A.E. Elhabashy, L.J. Wells, J.A. Camelio, W.H. Woodall, A cyber-physical attack taxonomy for production systems: a quality control perspective, J. Intell. Manuf. (2018) 1–16.
[31] L.D. Sturm, C.B. Williams, J.A. Camelio, J. White, R. Parker, Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the. STL file with human subjects, J. Manuf. Syst. 44 (2017) 154–164.
[32] W. Li, L. Xie, Z. Deng, Z. Wang, False sequential logic attack on SCADA system and its physical impact analysis, Comput. Secur. 58 (2016) 149–159.
[33] J. Fruhlinger, What is Stuxnet, who created it and how does it work?, CSO Online. (2017). https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html (accessed February 18, 2019).
[34] S. Karnouskos, Stuxnet worm impact on industrial cyber-physical system security, in: IECON 2011-37th Annu. Conf. IEEE Ind. Electron. Soc., IEEE, 2011: pp. 4490–4494. http://ieeexplore.ieee.org/abstract/document/6120048/.
[35] Robert M. Lee, Michael J. Assante, Tim Conway, ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper - German Steel Mill Cyber Attack, 2014.
[36] W. Yakowicz, Honda Factory Shuts Down After WannaCry Virus Infects Computers, Inc.Com. (2017).
[37] D. Wu, A. Ren, W. Zhang, F. Fan, P. Liu, X. Fu, J. Terpenny, Cybersecurity for digital manufacturing, J. Manuf. Syst. (2018).
[38] F. Imani, A. Gaikwad, M. Montazeri, P. Rao, H. Yang, E. Reutzel, Layerwise in-process quality monitoring in laser powder bed fusion, in: ASME 2018 13th Int. Manuf. Sci. Eng. Conf., American Society of Mechanical Engineers, 2018: p. V001T01A038–V001T01A038.
[39] M. Yampolskiy, L. Schutzle, U. Vaidya, A. Yasinsac, Security challenges of additive manufacturing with metals and alloys, IFIP Adv. Inf. Commun. Technol. 466 (2015) 169–183.
[40] M.R. Yavari, K.D. Cole, P. Rao, Thermal Modeling in Metal Additive Manufacturing using Graph Theory, J. Manuf. Sci. Eng. (2019) 1–71.
[41] S.R. Chhetri, A. Canedo, M.A.A. Faruque, KCAD: Kinetic Cyber-attack Detection Method for Cyber-physical Additive Manufacturing Systems, in: Proc. 35th Int. Conf. Comput.-Aided Des., ACM, New York, NY, USA, 2016: pp. 74:1–74:8.
[42] E. Malekipour, H. El-Mounayri, Common defects and contributing parameters in powder bed fusion AM process and their classification for online monitoring and control: a review, Int. J. Adv. Manuf. Technol. 95 (2018) 527–550.
[43] M. Montazeri, R. Yavari, P. Rao, P. Boulware, In-process monitoring of material cross-contamination defects in laser powder bed fusion, J. Manuf. Sci. Eng. 140 (2018) 111001.
[44] R. Caprihan, A. Kumar, K.E. Stecke, Evaluation of the impact of information delays on flexible manufacturing systems performance in dynamic scheduling environments, Int. J. Adv. Manuf. Technol. 67 (2013) 311–338.
[45] H. Bouzary, F.F. Chen, Service optimal selection and composition in cloud manufacturing: a comprehensive survey, Int. J. Adv. Manuf. Technol. (2018) 1–14.
[46] K. Krishnaiyer, F.F. Chen, H. Bouzary, Cloud Kanban Framework for Service Operations Management, Procedia Manuf. 17 (2018) 531–538.
[47] H. Bouzary, F.F. Chen, A hybrid grey wolf optimizer algorithm with evolutionary operators for optimal QoS-aware service composition and optimal selection in cloud manufacturing, Int. J. Adv. Manuf. Technol. 101 (2019) 2771–2784.
[48] H. Vincent, L. Wells, P. Tarazaga, J. Camelio, Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems, Procedia Manuf. 1 (2015) 77–85.
[49] Virus outbreak at iPhone chip plant could delay shipments, ComputerWeekly.Com. (n.d.). https://www.computerweekly.com/news/252446344/Virus-outbreak-at-iPhone-chip-plant-could-delay-shipments (accessed February 15, 2019).
[50] RISI - The Repository of Industrial Security Incidents, (n.d.). https://www.risidata.com/Database/Detail/reverse-osmosis-system-plc-attacked (accessed February 19, 2019).
[51] E.A. Harris, Data Breach Hurts Profit at Target, N. Y. Times. (2017). https://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html (accessed February 19, 2019).