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.

Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach

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

This paper presents a novel approach using game theory to assess the risk likelihood in manufacturing systems quantifiably. Cybersecurity is a pressing issue in the manufacturing sector. Nevertheless, managing the risk in cybersecurity has become a critical challenge for modern manufacturing enterprises. In risk management thinking, the first step is to identify the risk, then validate it, and lastly, consider responses to the risk. If the risk is below the security risk appetite of the manufacturing system, it could be accepted. However, if it is above the risk appetite, the system should appropriately respond by either avoiding, transferring, or mitigating the risk. The validation of the risk in terms of severity and likelihood of the threat, however, is challenging because the later component is hard to quantify. In this paper, Failure Modes and Effects Analysis (FMEA) method is modified by employing game theory to quantitatively assess the likelihood of cyber-physical security risks. This method utilizes the game theory approach by modeling the rivalry between the attacker and the system as a game and then try to analyze it to find the likelihood of the attacker's action. We first define players of the game, action sets, and the utility function. Major concerns of cyber security issues in the manufacturing area are carefully considered in defining the cost function composed of defense policy, loss in production, and recovery. A linear optimization model is utilized to find a mixed-strategy Nash Equilibrium, which is the probability of choosing any action by the attacker also known as the likelihood of an attack. Numerical experiments are presented to further illustrate the method. Forecasting the attacker's behavior enables us to assess the cybersecurity risk in a manufacturing system and thereby be more prepared with plans of proper responses.

Keywords: Game Theory; Cybersecurity in Manufacturing; Risk Assessment;

1. Introduction

New technological advances in manufacturing systems, such as industry 4.0 [1], cloud manufacturing [2], and real-time service composition [3,4] has opened a new horizon for the manufacturing world. However, the integration of the cyber systems with the traditional physical manufacturing exposes these systems to a new type of risks that was unknown beforehand [5,6]. Even though most of these threats are not unique for manufacturing systems, the immaturity of manufacturing systems towards cybersecurity in comparison with other sectors such as banking and utility is made the effort sensitive. Several incidents in the past decade showed the devastating impact that cybersecurity threat could cause to manufacturing systems [7].

National Institute of Standards and Technology (NIST) [8] developed a cybersecurity framework to reduce cybersecurity risk for manufacturers. This framework consists of identify, protect, detect, respond, and recover. The first step on this procedure is to identify and assess the risks in manufacturing systems that can be done by standard procedures such as ISO 27000 [9] which is the application of Failure Modes and Effects Analysis (FMEA) techniques to the analysis of information security risks. Inspiring form general FMEA method and ISO27k in this paper identified risks are assessed by calculating cybersecurity criticality numbers (CSCN), which is the product of severity and likelihood of occurrence. If the calculated number for each risk is below the risk appetite (i.e., the acceptable risk limit) of the system, it could be accepted. However, if the number is above the risk appetite, it should be appropriately responded by either avoiding, transferring or mitigating the risk.

Nevertheless, the challenge here is to determine the second component to calculate the CSCN when there is no prior experience for specific risk in a system. Moreover, another problem associated with this method is ignoring the fact that the relation between the attacker and the system is not a static interaction and the attacker will respond to the new strategy of the system, which was chosen based on FMEA assessment, accordingly. Unlike the general failures in mechanical systems, the cause of cybersecurity failures could vary for different situation since they incorporate with human contributors. So it is necessary to consider the dynamic interaction of the attacker and the system when calculating the likelihood of occurrence.

This paper proposes a novel approach to provide manufacturing system insight into their potential cybersecurity risks through utilizing game theory approach. The interaction of the attacker and the system will be assumed as a game in which each player intend to increase their gain from the game and hence each player react to the opponent's strategy accordingly. In this method, the strategy of the attacker in the long run, Nash equilibrium, will be considered as the likelihood of a risk, which enables us to manage risks quantitatively.

The rest of the paper is organized as follow. In section 2, related work in the field of vulnerability and risk assessment in manufacturing systems is reviewed. Section 3 discusses the proposed method by elaborating the theory to quantify the risk, formation of the game and the method to analyze it. Section 4 presents a numerical example to further illustrate the proposed method. In section 5, the results of the case study are discussed, and finally, section 6 concludes the paper and provides suggestions for future works.

2. Literature review

Unlike the other sectors such as utility [10], transportation [11], and healthcare [12,13], manufacturing systems are not mature enough towards the cybersecurity threats. There exists only limited research in the field of cybersecurity risk assessment in manufacturing systems. Desmit et al. [14] proposed a systematic approach to identify cyber-physical vulnerabilities in intelligent manufacturing systems using intersection mapping to identify vulnerabilities and then analyzing the impact of cyber-physical vulnerability with decision trees. Hutchins et al. [15] establish a framework that provides a mechanism for identifying generic and manufacturing-specific vulnerabilities considering data flows within a manufacturing system and its supply chain.

To quantifiably measure the consequences of cyber-attack on a manufacturing enterprise, Prabhu et al. [16] develop two essential metrics, Damage Index (DI) and Vulnerability Index (VI). Moreover, Zarreh et al. [17,18] assume the interaction of attacker and manufacturing enterprise as a game and proposed a framework to assess the repercussions of a cyber-physical thereat and choose a proper method to defend. Utilizing the same mindset, Bracho et al. [19,20] introduces a simulation-based model to assess the consequences of manufacturing systems' performance under the presence of cybersecurity risks.

Because of the increasing popularity of additive manufacturing, several researches concentrate on vulnerabilities of this domain and try to suggest some countermeasures to mitigate the attacks. Zeltmann et al. [21] highlight the risk of alteration of direction in 3D printing on the mechanical behavior of a specimen as a result of a cyber-attack. Padmanabhan and Zhang [22] propose a different framework to assess cybersecurity vulnerabilities in additive manufacturing using the metrics, namely, loss of information, inconsistency, relative frequency, lack of maturity and time until detection for each stage of the process.

Other researches try to recommend defense policies to enhance the security of manufacturing systems. Wu et al. [23] establish a cyber manufacturing system testbed to enable simulation and data collection for investigating cyber manufacturing security. Li et al. [24] propose a cloud-based system to share knowledge for injection mold redesign (IMR). They utilize blockchain technology to securely implement standards and protocols. Vincent et al. [25] recommend a product/process design approach to detect attacks in real-time to compensate for the shortcomings of quality control systems in cyber-physical manufacturing systems.

3. Model

3.1. Quantifying risks

To quantifiably assess risks in a system, a method similar to the failure mode and effective analysis (FMEA) in the manufacturing system is employed. In this method cybersecurity criticality number (CSCN) is considered to decide if a risk is critical and should be responded to adequately. As equation (1) shows, cybersecurity criticality number (CSCN) depends on two elements, severity of the risk if it happens and the likelihood of occurrence of this risk. In this method, the risk is a severe threat when CSCN is high meaning both the severity and the likelihood of occurrence of risk is relatively high, and the system needs to respond as its first priority. On the second priority when CSCN is low while the severity is high the risk should get attention since the consequence of the risk is high. On the next priority, the system could respond to those risk with low CSCN with low severity and high likelihood. At last, risks with low CSCN while both severity and likelihood are low needs no attention.

$$CSCN = Severity(S) \times Likelihood(L) \tag{1}$$

The severity of risk is assigned a numerical value between 1 and 10 based on criteria in Table 1, where 10 is the most severe threat, and 1 is for a threat with no consequences and effects. The table is proposed based on ISO27k, and it could be customized based on the needs and concern of a manufacturing enterprise.

Table 1. Severity Table

Severity	Effect	Description	Severity	Effect	Description
10	Catastrophic	Irreversible damage to manufacturing enterprise or its reputation	5	Low	Disruption of production, Major violations of process
9	Extreme	The manufacturing system negatively affected, likely to reverse back to the original value in over 5 days	4	Very Low	Disruption of production, Major violations of procedures
8	Very High	The manufacturing system negatively affected, likely to reverse back to the original value between 3-5 days	3	Minor	Disruption of production, Minor violations of policies
7	High	The manufacturing system negatively affected, likely to reverse back to the original value between 1-3 days	2	Very Minor	Minor violation of procedures, production continuity not affected
6	Moderate	The manufacturing system negatively affected, likely to reverse back to the original value within 1 day	1	None	No effect whatsoever

Similarly, the likelihood of occurrence can be assigned from a range of 1 to 10 listed in Table 2 in which the 10 is for a threat with probability of occurrence higher than 90% and 1 is for one with probability of occurrence less than

10%. For FMEA, this probability typically comes from past experiences of the system or related systems. However, for cybersecurity, often there is a lack of relevant prior experiences. In some cases, it may not be appropriate to generalize similar incident to calculate the probabilities because of dissimilarity in the background of the incidents in different systems. Furthermore, data collection is a challenging effort in its nature, especially in the case of cybersecurity since many companies try to hide their vulnerabilities and incidents on their system to prevent harm to their reputation.

To overcome this challenge, this paper recommends utilizing game theory approach to forecast the likelihood of attacks and use the attacker's strategy (in the form of probability) to quantitatively assign the likelihood of occurrence in risk management thinking.

Table 2. Likelihood of occurrence

Occurrence	Description	Occurrence	Description
10	Likely to occur in 90-100% of experiences	5	Likely to occur in 40-50% of experiences
9	Likely to occur in 80-90% of experiences	4	Likely to occur in 30-40% of experiences
8	Likely to occur in 70-80% of experiences	3	Likely to occur in 20-30% of experiences
7	Likely to occur in 60-70% of experiences	2	Likely to occur in 10-20% of experiences
6	Likely to occur in 50-60% of experiences	1	Likely to occur in 0-10% of experiences

3.2. Game Formation

To predict the attackers' behavior through the game theory approach, firstly the main tenets of the game should be identified and then by analyzing it the probability of attacker's actions named strategy of attackers could be found. The three primary tenants of a game are players, actions and a reward function. The formation of the game in this paper is based on published work [17,18], where more information about this game theory approach in cyber security of manufacturing systems can be found.

The first element of the game is to identify the players of the game, in this paper the game is considered to be a two player game, i.e., attacker and defender. The attacker could be single hacker, group of hackers, terrorist group or unfriendly government. On the other side, there will be a defender which in this paper is a manufacturing system that attempts to minimize the damage to its system through playing the game optimally.

The second element of the game is an action set for each player. On the attacker side, any vulnerability or weaknesses in the system can be exploited by the attacker. For the defender, any possible defense mechanism to prevent, minimize or mitigate an attack action will be considered as an action for the defender.

Lastly, the third element of the game is the utility function for a manufacturing system. The function includes: (1) cost of maintaining a security policy which is the cost to keep the defense system up and running, (2) direct and indirect costs of production losses, and (3) cost of recovery incurred by the amount of time, effort and money paid to bring back the system to its safe initial running state. The utility (reward) function of the two-player game is formulated by an $n \times m$ matrix where n is the number of actions by attackers and m is the number of actions by the defender, as shown below [18]:

$$\Gamma\left(a_k, d_l\right) = s_{d_l} - \left(s_{a_k} \times e_{a_k,d_l}\right) + T \times p_{a_k} \times \left(1 - e_{a_k,d_l}\right) + r_{a_k} \times \left(1 - e_{a_k,d_l}\right) = \begin{pmatrix} \gamma_{11} & \cdots & \gamma_{1m} \\ \vdots & \gamma_{a_k,d_l} & \vdots \\ \gamma_{nm} & \cdots & \gamma_{nm} \end{pmatrix}, \forall\, a_k, d_l \tag{2}$$

3.3. Analysis of the Game

There are numbers of ways to analyze such a model as a game such as linear programming, Markov decision processes (MDP), quantal respond equilibrium (QRE), minimax-Q, and Q-learning. Regardless of the analyzing method, the main goal is to find the strategy of the attacker which is the key to quantify the likelihood of occurrence and calculate CSCN. Based on the definition, Strategy of a player is a set of probabilities of utilizing any action in action set for any players, and it can be shown as below for both players, where $\pi(a_i)$ is the probability that the attacker will use attack action a_i. Similarly, $\varphi(d_j)$ is the probability that defense action d_j will be adopted by the defender.

$$\pi(a_i) = \{\pi(a_1), \pi(a_2), \ldots, \pi(a_n)\}, \quad \sum_{i=1}^{n}\pi(a_i)=1$$
$$\varphi(d_j) = \{\varphi(d_1), \varphi(d_2), \ldots, \varphi(d_m)\}, \quad \sum_{j=1}^{n}\varphi(d_j)=1 \tag{3}$$

The strategy of a player in the long run could be found by formulating the optimization problem as a linear program to find the optimal global utility. The global utility is the amount of damage to the system or the win for the attacker in the long run. This number is directly related to the strategy of both players, and by altering the strategy, the value will change accordingly. Consequently, it is assumed in this research that any player will try to maximize the gain by altering his strategy regardless of the strategy of the other player. Based on this intuition the problem if formulated to find a profile of strategies such that each player's strategy is the best response (results in the highest available payoff) against the equilibrium strategies of the other players. This equilibrium is called the Nash equilibrium.

$$U(\pi^*, \varphi^*) = \arg\min\max U_{ij}(\pi(a_i), \varphi(d_j), \gamma_{ij}) \tag{4}$$

Additionally, the game is defined as a two-player zero-sum game with complete information and rational players. Further details of the solution approach can be found in [17,18].

4. Numerical Example of Risk Assessment

In this section, a numerical case study is presented to further illustrate the proposed method. The manufacturing system considered in this example identifies seven risks, namely, theft of intellectual properties, hacking employee log-in credentials, infecting SCADA, hacking wireless devices, taking over production machines, infecting network, insider attack, in its cyber-physical system. Any attempts to harm and attack these vulnerabilities would be considered as actions from the attacker. On the other side, the manufacturing system as the defender has five different actions to react to the attacker's actions. These actions could be from the four main types of defensive response which is to avoid, transfer, mitigate or accept the risk. Doing nothing is considered as the last available action for defender, *D5*, which is an acceptable type of response for the defender. The summary of the model is presented in Table 3.

Table 3. Summary of system information used in the illustrative example.

Type of game	Two players zero-sum game with incomplete information and rational players
Players	Two players: Attacker and the system as the defender
Attacks	$A = \{a_1, a_2, a_3, a_4, a_5, a_6 a_7\}$ = *{theft of intellectual properties, hacking employee log-in credentials, infecting SCADA, hacking wireless devices, taking over production machines, infecting network, insider attack }* where a_k denotes an attack action
Defenses	$D = \{d_1, d_2, d_3, d_4, d_5\}$={avoid risk, transfer risk, mitigate risk, accept risk, do nothing} where d_l denotes a defender action
Maintaining cost of defense mechanism	$s = \{80, 150, 200, 500, 0\}$ where s_l denotes maintenance cost for d_l
Production loss rate	$p = \{0.1, 0.15, 0.8, 0.5, 1, 0.1, 1\}$ where p_k denotes the production loss rate according to a_k
Total production	$T = 1000$
Cost of recovery	$r = \{140, 50, 100, 300\}$ where r_k denotes the cost of recovery from attack a_k to bring back the system to its initial state
matrix of effectiveness	$E = \{e_{a_i,a_{-i}}\} = \begin{bmatrix} 0.8 & 0.1 & 0.1 & 0.3 & 0 \\ 0.95 & 0.1 & 0.1 & 0.3 & 0 \\ 0.1 & 0.7 & 0.5 & 0.9 & 0 \\ 0.1 & 0.85 & 0.95 & 0.7 & 0 \\ 0.2 & 0.7 & 0.8 & 0.9 & 0 \\ 0.4 & 0.85 & 0.95 & 0.1 & 0 \\ 0.05 & 0.8 & 0.2 & 0.2 & 0 \end{bmatrix}$

The interaction between the system and the attacker is modeled as a two-player zero-sum game. This game is a simultaneous stochastic game meaning both players choose their action in the same time or if one player plays sooner, the other player will not able to know its move until it chooses an action too. Also, this is a game with the complete

information and rational players which mean that both players know the consequence of their actions and both are trying to gain a maximum benefit from the game. Based on the definition of the game since it is a zero-sum game the maximum gain for the defender is to minimize damage to the system.

Having the action sets for both players defined and knowing the maintaining cost of defense, production loss rate, total production, cost of recovery, and effectiveness matrix, the utility function (reward function) can then be calculated by Equation (2). As mentioned before, since the game is a two-player game, the utility function could be shown as a 7×5 matrix where rows represent the attack actions and columns represent defender. In this function, each element demonstrates the gain of the attacker from the joint action of both players. Since the game is defined as a zero-sum game, negative values indicate a defender loss and an attacker gain.

$$\Gamma = \begin{bmatrix} 64 & 351 & 396 & 518 & 240 \\ 14 & 315 & 360 & 490 & 200 \\ 1080 & 381 & 660 & 162 & 1120 \\ 657 & 120 & 42.5 & 345 & 650 \\ 960 & 381 & 264 & 162 & 1120 \\ 228 & 67.5 & 25 & 720 & 300 \\ 1501 & 330 & 1360 & 1600 & 1500 \end{bmatrix} \tag{5}$$

Now based on the utility function, the Nash equilibrium could be calculated. There are numbers of ways to find the Nash equilibrium for such a game, but since the game is zero-sum with two players and target is to find equilibrium, the best to use linear programming [18]. In this example, strategies found for each player are as follows:

$$\begin{aligned} \pi(A_i) &= \{\pi(A_1),\ \pi(A_2),\ \ldots,\ \pi(A_n)\} = \{0,\ 0,\ 0.46,\ 0,\ 0.39,\ 0,\ 0.15\} \\ \varphi(D_j) &= \{\varphi(D_1),\ \varphi(D_2),\ \ldots,\ \varphi(D_m)\} = \{0,\ 0.87,\ 0,\ 0.13,\ 0\} \end{aligned} \tag{6}$$

As seen, the attacker abandons using actions A1, A2, A4, and A6 in the long run and adopts the strategy of using A3, A5, and A7 with the probability of 46%, 39%, and 15% respectively. Similarly, the defender ends up abandoning D1, D3, and D5 and only uses D2 and D4 with the probability of 87% and 13%, respectively. Ultimately, the global utility, which means the amount that the attacker will gain and the defender will lose in the long run, is 373.50 and there will be no better strategy for them to maximize further their utility and any deviation from these strategies will cost the player lower gain in the long run.

In assessing the likelihood of occurrence, risks (types of attack) with zero probability are assigned with a likelihood score of 1, according to Table 2. Similarly, the likelihood of risks with non-zero probability could be found from the same table. Now, by knowing the severity and having the likelihood calculated of each risk, the cybersecurity criticality number (CSCN) could be found by the multiplication for each risk (Equation 1).

Table 4. Cybersecurity criticality number results for system's vulnerabilities

Attack Action		Severity (S)	Likelihood (L)	CSCN
Theft of intellectual properties	A1	7	1	7
Hacking employee log-in credentials	A2	4	1	4
Infecting SCADA	A3	8	5	40
Hacking wireless devices	A4	5	1	5
Taking over production machines	A5	6	4	24
Infecting network	A6	5	1	5
Insider misuse	A7	7	2	14

5. Risk Management based on CSCN

Every company should have a threshold for their risk appetite which means any risk with CSCN above the risk appetite of the company should be responded. To have a better understanding, in this example the four zones are

explained, minor risk zone, low-risk zone, high-risk zone, and extreme risk zone. However, the main criteria to decide is the risk appetite of the company.

It is assumed that the risk appetite of the company is below 30. Moreover, any risk with the cybersecurity criticality number below 10 will be accepted which illustrate the minor risk zone, and there would be no need to react. Similarly, any risk with cybersecurity criticality number above 50 illustrates the extreme risk zone and should be addressed immediately as both the severity and likelihood are high. Any risk between 10 and 30 will be considered as low risk and between 30 and 50 is considered as the high-risk zone. These limits are shown with three cures in Figure 1 that illustrate calculated CSCN for all the risks in terms of severity vs. likelihood.

As Figure 1 and Table 4 illustrate the only risk with CSCN above the company's risk appetite is A3, infection of SCADA and control systems, with the CSCN of 40 which is in the high-risk zone. It is mostly due to the high severity of the risk besides having the highest probability of occurrence among the set of risks since it is aligned with the strategy of the attacker in the long run. Besides the vulnerability of the control systems in the company, another two risks, A5 (taking over production machines) and A7 (insider misuse) have relatively high CSCN but are located in low-risk zone. It means that since their CSCN is below the risk appetite of the company, 30, they should be monitored but could be accepted. Rest of the risks, A1, A2, and A4, have a cybersecurity criticality number below 10, which means they are in the low-risk zone and no action needed for them.

According to the analysis mentioned above, the company should react to the A4 by introducing new defensive action, and upon completion, the procedure of risk assessment should be done again. This procedure should be repeated until all the risks come below the risk appetite of the company. There is a point that should be considered here that changing defense policy to lower the risk of A4 will change the whole formation of the game and attacker will respond accordingly. It means that for the next round of the analyses, those risks with high severity could get a high likelihood and as a result, the priority of addressing risk would be different.

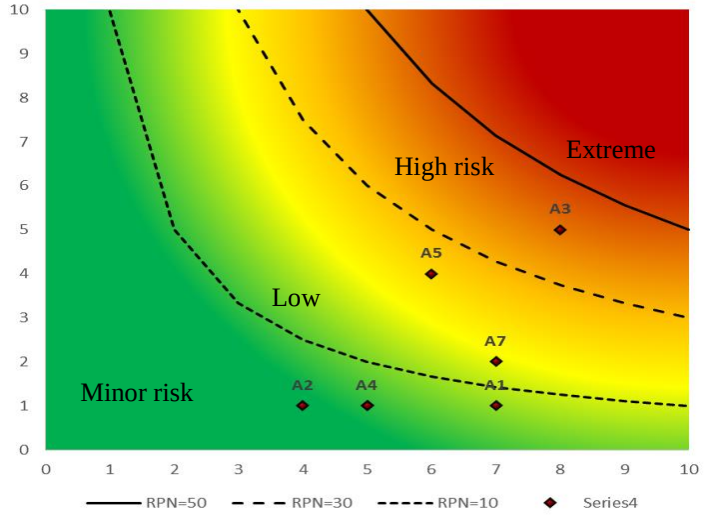

Figure 1. Cybersecurity criticality number (CSCN) in terms of severity vs. likelihood

6. Conclusion

The ISO defines risks as the effect of uncertainty on an object, or anything that could go wrong in the company. Recently, as a result of the integration of cyber systems and physical production systems, manufacturing enterprises are exposed to a new type of risks from cybersecurity. Failure modes and effects analysis (FMEA) provides a method to assess risks in manufacturing systems however it has shortcoming regarding cybersecurity including its weakness when there is an insufficient prior experience to find the likelihood of occurrence and also not considering the dynamic interaction of attacker and the system toward the cybersecurity.

In this paper, a method was proposed that employed game theory approach to facilitate cybersecurity risk assessment by considering the interaction of an attacker and a manufacturing enterprise as a game to predict the attackers' behavior probability in the long run also known as Nash equilibrium mixed-strategy of the attacker. Then,

cybersecurity criticality number (CSCN) was proposed as the product of severity and likelihood of occurrence as the criteria to assess cybersecurity risks comparing to risk appetite of the system. Also, severity table is modified to match the needs of a manufacturing system regarding the cybersecurity issues. Also, a numerical case study was presented to further demonstrate the proposed method.

For future research, the first suggestion is to refine the utility function of the game to consider further important detail and characteristics in the manufacturing setting. For example, the impact of social costs such as harm to the reputation of a company due to an attack could be considered. Also, the game could be modeled as a non-zero-sum game that needs to have two utility functions, one for the defender and one for the attacker. The current function only considers the characteristics of the defender which could be different from the attacker's perspective. Besides, the amount of the loss for the defender does not always equal to the gain for the attacker.

References

[1] E. Hofmann, M. Rüsch, Industry 4.0 and the current status as well as future prospects on logistics, Comput. Ind. 89 (2017) 23–34.
[2] K. Krishnaiyer, F.F. Chen, H. Bouzary, Cloud Kanban Framework for Service Operations Management, Procedia Manuf. 17 (2018) 531–538.
[3] H. Bouzary, F.F. Chen, Service optimal selection and composition in cloud manufacturing: a comprehensive survey, Int. J. Adv. Manuf. Technol. (2018) 1–14.
[4] H. Bouzary, F.F. Chen, K. Krishnaiyer, A modified discrete invasive weed algorithm for optimal service composition in cloud manufacturing systems, Procedia Manuf. 17 (2018) 403–410.
[5] DBIR: Understand Your Cybersecurity Threats, Verizon Enterp. Solut. (2017).
[6] M. Amini, S. Chang, Assessing Data Veracity for Data-Rich Manufacturing, in: IIE Annu. Conf. Proc., Institute of Industrial and Systems Engineers (IISE), 2017: pp. 1661–1666.
[7] D. Albright, P. Brannan, C. Walrond, Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? | Institute for Science and International Security, (n.d.). http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.
[8] K. Stouffer, K. Stouffer, T. Zimmerman, C. Tang, J. Lubell, J. Cichonski, J. McCarthy, Cybersecurity framework manufacturing profile, US Department of Commerce, National Institute of Standards and Technology, 2017.
[9] ISO/IEC 27001 Information security management, ISO. (n.d.). http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/isoiec-27001-information-securit.html (accessed February 10, 2019).
[10] U.P.D. Ani, H. He, A. Tiwari, Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective, J. Cyber Secur. Technol. 1 (2017) 32–74.
[11] 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.
[12] 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.
[13] B. Malmir, M. Amini, S.I. Chang, A medical decision support system for disease diagnosis under uncertainty, Expert Syst. Appl. 88 (2017) 95–108.
[14] 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.
[15] M.J. Hutchins, R. Bhinge, M.K. Micali, S.L. Robinson, J.W. Sutherland, D. Dornfeld, Framework for identifying cybersecurity risks in manufacturing, Procedia Manuf. 1 (2015) 47–63.
[16] V. Prabhu, J. Oyekan, S. Eng, L.E. Woei, A. Tiwari, Towards Data-Driven Cyber Attack Damage and Vulnerability Estimation for Manufacturing Enterprises, in: Int. Conf. Remote Eng. Virtual Instrum., Springer, 2018: pp. 333–343.
[17] 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.
[18] 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.
[19] 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.
[20] 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.
[21] 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.
[22] A. Padmanabhan, J. Zhang, Cybersecurity risks and mitigation strategies in additive manufacturing, Prog. Addit. Manuf. (2018) 1–7.
[23] M. Wu, J. Song, L.W. Lucas Lin, N. Aurelle, Y. Liu, B. Ding, Z. Song, Y.B. Moon, Establishment of intrusion detection testbed for CyberManufacturing systems, Procedia Manuf. 26 (2018) 1053–1064.
[24] Z. Li, L. Liu, A.V. Barenji, W. Wang, Cloud-based Manufacturing Blockchain: Secure Knowledge Sharing for Injection Mould Redesign, Procedia CIRP. 72 (2018) 961–966.
[25] 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.