Security Perspective in RAMI 4.0

Amr I. Elkhawas,

Information Security - School of Communication and Information Technology, Nile University, Egypt
a.elkhawas@nu.edu.eg

Marianne A. Azer,

National Telecommunication Institute, Nile University, Egypt
mazer@nu.edu.eg

Abstract— **Cloud Computing, Internet of Things (IoT) are the main technologies contributing to the adoption of the fourth revolution in manufacturing, Industry 4.0 also known as smart manufacturing or digital manufacturing. Smart manufacturing facilitates and accelerates the process of manufacturing with the connection of all the systems related to the manufacturing process starting with the Enterprise Resource Planning (ERP) systems, the Industrial Control Systems (ICSs) which control the production line and the Cyber Physical Systems (CPSs). Before the emerging of web applications, cloud applications and thin clients, ICSs and CPSs were already present but the protocols used for those systems were not designed for the Internet. In this paper, we tackle the security challenges that are accompanied by the emerging of this new technology, the mitigation techniques and the governance and compliance issues associated with it.**

Keywords **— Industrial Control Systems, Industry4.0, IoT, RAMI 4.0, Security Challenges, Smart Manufacturing.**

I. INTRODUCTION

With the emergence of the new revolutionary manufacturing approach several security challenges commence. The fourth industrial revolution Industry 4.0 arose due to the vast adoption of IoT systems, cloud computing, and the vast demand for the digitization of the world. Also known as smart manufacturing, the interconnection of these infrastructure systems from the resource management of the production line, and the ICSs which automates the production process, and the CPSs which are the actual manufacturing machines used to physically manufacture the product is the main concept of this trend. Whether this approach is used in nuclear power plants, water treatment systems or even a production line for consumer goods, any modification to the controls of the system or production line can have catastrophic repercussions. There are not enough robust guidelines for implementing these systems securely. The security risks must be highlighted to be implemented in the Reference Architecture Model for Industry 4.0 (RAMI 4.0). After listing these challenges, contributions to RAMI 4.0 from the security perspective are needed, especially after the understanding the risks and the predicted consequences from such threats.

In this paper, we list the common security challenges accompanied by the adoption of this emerging technology along the mitigation techniques and the need to revise the RAMI 4.0 standard from the security perspective. The remainder of this paper is organized as follows. In section II, we explain the RAMI 4.0, section III, we present the common security challenges and mitigation techniques. Section IV illustrates a developed process model that provides a semi-automated threat and risk analysis system for Small and Medium Enterprises (SMEs). Finally, in section V, conclusions and future work are presented.

II. RAMI 4.0

In 2015, the "Platform 4.0" developed the so-called Reference Architecture Model for Industry 4.0 (RAMI 4.0). [1] RAMI 4.0 is a three-dimensional layered model, the first axis is the architecture axis, which consists of six unique levels: Assets, integration, communication, information, functional, and business layers. Detailing the above levels with a bottom up approach, the bottom layer is the "Asset" layer, which actually represents the physical and non-physical layers. Each component or function of the upcoming layers must be affiliated to an object of the asset layer. The "Integration" layer consists of computerized interaction between the physical layer and the users or software. It mainly falls underneath the umbrella of Information Technology (IT). For example, the Human Machine Interface (HMI) falls in the "integration" layer which provides a means of controlling the physical asset which in this case is the ICS. The "Communication" layer on the other hand, is to facilitate the communication between the different components of the system, providing the means to control the "Integration" layer. As for the "Information" layer, the processing of the events occurs. For this purpose, data integrity is a must. The "Functional" layer is the runtime environment for services and applications. It is where all the functions, applications and systems intersect, it can be considered the brain of the system, in which operations are scheduled or altered due to the acquisition of certain data from the above layers. Lastly, the "Business" layer provides the bigger picture. The abstract business model is the result from all the above layers of planning an operating.

The second axis is the "Life Cycle and Value Stream" layer represented in IEC 62890. It represents the lifetime of an asset and the value-added process. It is divided into two specific areas, the product type and the product instance. The type is already present from the initiation of the product idea and covers the phases from the ordering to the product prototype. The instance is spawned after the evolution from a prototype to production, after all testing has been done on the product. The produced end product is then called an instance. Types, along with instances can be divided into two sub phases development and maintenance/usage for the types, while they

are divided for the latter into production and maintenance/usage.

The last axis of the RAMI 4.0 model is the "Hierarchy Levels" layer, consisting of products, field devices, control devices, stations, work units, enterprises and connected world which align functional models to specific levels. This model is depicted in Figure 1[1].

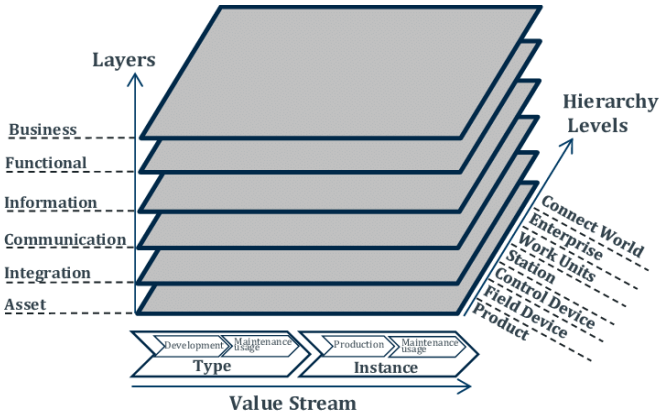

Figure 1: RAMI 4.0 structure [1]

To further explain the "Hierarchy Level", each level will be tackled individually. The first level is the "Products" level, which includes the products that are able to initiate communication; they fall under the category of active elements within the production system. They provide information on their individual properties and necessary production steps. Next, the "Field Device" level includes digital devices such as sensors and actuators, the level "Control Device" contain controllers and embedded controllers. Production machines and smart logistics vehicles are located at the "Station" level. Production plants and departments within a company are at the "Work Centers" level. The "Enterprise" level tackles the whole company and last but not least the "Connected World" level represents its outside networks, for example, business partners and customers, including cloud services [2] [3] [1].

III. Security Challenges and Mitigation Techniques

The IoT trend has played an immense role in the adoption of the fourth industrial revolution. Accordingly, there are a set of challenges Industry 4.0 might face in order to be widely implemented. The following are a set of facilitators that will help overcome the challenges ahead of it.

Smart networking: Most systems including internal logistics, operating supplies and automated systems are usually connected through wireless communication technologies. These ease the accessibility of the operated system, Software Defined Networking (SDN) is a technology that facilitates the connection of these systems in a "Plug and Play" manner.

Mobility: This allows the use of cloud-based platforms that can control the entire system from end to end, report on failures and maintenance issues, and connect the user with end customers and suppliers in a practical and efficient way. The adopters must stray away from the proprietary communication methods and protocols and adopt an open source method of communication for interoperability and flexibility between all the different devices. This allows customers to integrate with the whole supply chain, to customize their requirements individually. All the above advances in technology do not come without security challenges [4] [5] [6] [7]. In the following, we present several types of attacks.

i. Espionage

One of many security challenges is enterprise cyber espionage, confidential information and intellectual property theft due to the interconnection of these systems online across the internet. Black Vine is an example of hacking groups that are focused on targeting the industrial sector for intellectual property theft. They focus mainly on aerospace, energy and the healthcare industries. One of the attacks that are attributed to this group is the recent attack on the US Steel industry.

ii. Denial of Service

Another attack that is common to published services is the Denial of Service (DoS) attack. During this attack, a server is overwhelmed with a huge number of illegitimate requests that prevent the server from accepting and serving any other legitimate request subsequently leading to a DoS attack. This can cause a sensor to malfunction or even prevent an actuator from taking a desired action. Another vector of attacks is the supply chain and extended systems. These systems are prone to phishing attacks and credential theft resulting in massive data leakage [4] [5] [6] [7] [8] [9].

iii. Replay Attacks

In the replay attacks, valid packets are repeated or delayed serving a malicious purpose. For example, Byzantine replay attacks are when an attacker repeats packets that were captured previously between a sensor or actuator for example and the system controlling it at a certain desired time. Another replay attack is the wormhole attack, it is commonly found in wireless sensor networks, in which attackers can disrupt the routing protocol for instance to make a false representation of distance between two end points, and capture the packets going between them with the intent of replaying these packets in different regions [8] [10] [11].

iv. Deception Attacks

Deception attacks are also popular among CPSs, this is a type of attack in which the data integrity of the transferred packets is modified. For example, the Stuxnet worm can reprogram the code running on PLCs causing the systems to operate in an abnormal way. These types of attacks can also be named false data-injection attacks. [8] [12].

The authors in [13] took another approach to define the security issues in industrial IoT with a layered approach for the IoT system for the threat analysis model in Figure 2 [13]. Starting with the "Sensors and Actuators Layer", there are three kinds of attacks, tampering, eavesdropping and DoS. Tampering is when the attacker physically modifies the device. Eavesdropping is when an attacker gains access to the data transmitted by the device, this attack is a passive attack. If the packet is altered during transmission, then this becomes a replay attack as mentioned earlier. The infamous DoS attack is also an attack vector in this layer, as in most cases the IoT

devices communicate through radio access technologies in the physical layer which can be attacked by jamming and signal distortion. The sensors are not only prone to attacks but can also be the source of a Distributed Denial of Service (DDoS) attack, as their management access is particularly vulnerable due to poor deployment practices.

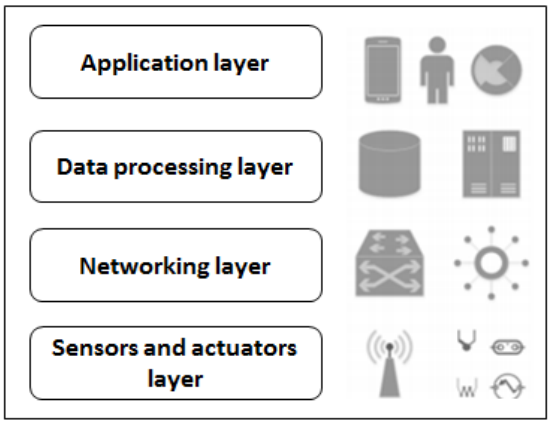

Figure 2: **The architectural layers of IoT systems [13]**

The Networking Layer is vulnerable to several attacks as follows. Exhaustion, where the networking resources **(**such as the buffer**)** are targeted with an attack specific to a resource. Collision, usually found in the wireless layer during the data transfer mechanism. It is considered a jamming attack in which it does not completely block transmissions, but causes degradation in data transmission performance. The above attacks can also contribute to another kind of attack called "Unfairness", in which the wireless sensor network's fairness mechanism is interrupted. This causes a slight denial of service that cannot be felt unless a large number of nodes in the system are targeted. Spoofed routing information is another method to attack the networking layer, which may consist of advertising wrong routes causing routing loops, shortened or extended routes. It can also contribute to selective forwarding in which certain packets are routed and others are intentionally dropped to corrupt the data transmission, this can also be called a sinkhole attack where the messages reach a destination and get blackholed. Wormhole attacks as mentioned are attacks in the network layer. Sybil attack, in which the attacker generates traffic from a multiple identity node to disrupt the fairness resources and redundancy present in the infrastructure. Finally, the "Flooding" attacks, mostly known as DDoS attacks that have immensely increased in magnitude after the adoption of IoT [13]. Exhaustion attacks are also present in the Data Processing layer, to interrupt the data processing of the IoT infrastructure. However, since the infrastructure is distrusted by nature, this attack has low impact on the system. Malware however has a high impact in this layer as it can be embedded in the data of IoT devices which can reach the cloud and datacentre if one of the peripheral nodes got infected.

Finally, the security issues at the application layer which include threats on the web client security measures as these devices are connected across the web they are vulnerable to web attacks. The communication method itself over the web can be compromised by either tampering with the data before reaching the configurable node, or by sniffing the traffic and getting a hold of confidential information. System integrity issues is also an issue, in which system should not fail in high activity stress, irregular process situations, computer or networking problems and incorrectly executed commands. Multi-user access and configuration editing should be regulated and logged so that multiple users cannot change the configuration at once and have the admin account approve the changes before committing the configuration change.

Sedghi et al. [14] mentioned that ICS networks and IT networks are different in nature and should be addressed that way when it comes to security. They have different performance requirements, reliability requirements, operating systems and applications. Therefore, they have different risk management and security goals and architecture. As a result of these differences, different priorities exist for these two networks as shown in Table 1 below [15].

Table 1: Difference in priorities in ICS and IT networks [15]

Priority	ICS	IT
Number 1	Availability	Confidentiality
Number 2	Integrity	Integrity
Number 3	Confidentiality	Availability

Knowledge of these priorities can assist in implementing the adequate operational and cybersecurity requirements. With the uprising of Industry 4.0, ICS security is a topic that all industrial actors must be familiar with and they should also understand the impact cyber-attacks can have on these systems. Common attacks consist of phishing, social engineering, compromise of domain controllers, attack on exposed servers, attack on ICS clients, session hijacking, piggybacking on the system's virtual private network, exploiting firewall vulnerabilities, misconfiguration of firewalls, forged Internet protocol addresses, bypassing the network security, physical access to the firewall, and sneaker net techniques. Degrees of damage can vary from downtime for ICSs and control equipment along with enterprise systems to catastrophic damage to the critical infrastructure that may lead to fatalities.

To give further awareness on the impact of cyber-attacks on the ICSs, a few publicly known incidents are listed below accompanied by the year of occurrence and their impact. In the year 2014, a blast furnace at a German steel mill was damaged severely as an aftermath of an attack on the plant's network. Ukraine, US and others, were targeted by a sophisticated malware specimen that targets and compromises the Human Machine Interfaces (HMIs) of several ICS vendors. The attack has focused on internet exposed HMIs to exploit vulnerabilities in the ICS software. Many other incidents were documented including the infamous attack on Saudi Arabia's Aramco Company that wiped thousands of computers clean and also the notorious "Stuxnet" attack on the Iranian nuclear centrifuges which was the first weaponized attack documented on ICSs.

Slammer worm was also one of the first documented attacks on ICS, in which it hit two major monitoring systems in a nuclear power plant in the United States in 2003, also another attack took place on a major transportation network's signal and dispatching system [14].

Attack Category	Layers Vulnerable	Attack Name	Description
Espionage	Application Layer	Phishing, Social Engineering, Malware, Eavesdropping	It is the act of obtaining intellectual property, secrets and information without the knowledge or consent of the information owner.
	Data Processing Layer		
	Networking Layer		
Denial of Service	Application Layer	Sybil Attack, DDoS, Malware, Slammer Worm	A server is overwhelmed with a large number of illegitimate requests that prevent the server from accepting and serving any other legitimate requests.
	Data Processing Layer		
	Networking Layer		
	Sensors and Actuators Layer		
Replay Attacks	Networking Layer	Wormhole attack	It is commonly found in wireless sensor networks, in which attackers can disrupt the routing protocol for instance to make a false representation of distance between two end points, and capture the packets going between them with the intent of replaying these packets.
	Sensors and Actuators Layer	Byzantine replay attack	It is when an attacker repeats packets that were captured previously between for example, a sensor or actuator and the system controlling it at a certain desired time.
Deception Attacks	Application Layer	False data-injection attacks, phishing, social engineering, session hijacking	Type of attack in which the data integrity of the transferred packet is modified. For example, the "Stuxnet" worm can reprogram the code running on the PLC to operate in an abnormal way.
	Sensors and Actuators Layer		

Table 2: A summary of attack categories, layer affected along with attack names and descriptions

Table 2 summaries common attacks, the layers it affects along with the attack names and descriptions. With all the above security challenges and previous incidents researchers started to look for ways to secure the Industry 4.0 systems, detect, monitor and mitigate these issues. Wegner et al. in [16] researched a specific point in the Industry 4.0 which is Computer Aided Manufacturing (CAM), in which they stated that the designs made by companies should be confidential, due to the considerable human effort spent on it, and organizations should solely take full benefit from it. They also specified that the integrity of these designs is a key to the manufacturing process, it must be transmitted to the manufacturing equipment in the exact format that it was on upon creation. Finally, it must be available to actually be produced at all, at any approved equipment across the globe. The concept of Industry 4.0 relies on the automation and communication of all the above processes without the need of human intervention. Thus, there is a need to secure these processes by authentication and authorization. In that case some questions need to be asked. For example: Is the request initiated to the manufacturing device authentic and is the user requesting that action authorized to do so? To address these issues, a concept called the "Comptroller Concept" was introduced. It is used to take input data, provide a key and store output data. This Manufacturing Security Enforcement Device (MSED) will be located on the manufacturing device or in close proximity to it, to cryptographically ensure the integrity of the transmitted data.

In [17], the authors developed a method to detect malicious code or malware running on ICSs. Since Programmable Logical Computers (PLCs) are a part of the ICSs that are used for monitoring and controlling the manufacturing process such as pumps, centrifuges, etc. and they perform the same tasks relatively throughout their lifetime, they are most likely to have a constant processing load and CPU usage almost all the time. Supervisory Control and Data Acquisition (SCADA) systems differ from PLCs in that they can control multiple sites over large distances. The signals are sent to Remote Terminal Units (RTU) and PLCs to convert the data and send it to the HMI to for the operators to observe or act upon. Malicious behaviour in these systems can be detected through the resource usage viewpoint (RUVi). RUVi's concept is that analysing the network traffic emitted from a device can provide information on the resource utilization of the computing devices and the operating systems that manage shared resources. Once the CPU utilization reaches around 70% the network traffic begins to exhibit deterioration because the CPU is too busy to handle networking efficiently.
Authors in [18] as well saw that protection from Advanced Persistent Threats (APTs) is also crucial for the adoption of Industry 4.0. Therefore, they proposed a solution to detect and react against APTs. This project called Advanced System for the Detection of Persistent Cyberattacks in Industry 4.0 (SADCIP) Project was funded by the Spanish Ministry of Economy, Industry and Competitiveness. The goals of this project were to investigate and analyze the common traits of

the most common cyber-attacks for Industry 4.0 environments, develop robust security standards and guidelines that touch not just upon security during the design phase but also deploy defense mechanisms to defend against this threat. This is in addition to creating an intrusion detection system to detect the existing cyber-attacks present in the Industry 4.0 architecture, and also developing detection systems to detect lateral movement and data exfiltration associated with APTs.

The authors in [19] suggested a solution in order to derive the type of the cyber-physical attacks that an Industry 4.0 system is undergoing, as well as a decision-making framework to determine if a certain security measure must be applied or if it is less costly to wait and gain further knowledge about the attack. Their proposal was based on a description language (CP-ADL) for cyber-physical attacks, with the use of XML patterns and a mathematical framework using the game theory.

Below is a list to explain cyber-physical attacks in six fields:

- *Method:* It represents the procedure employed to affect the system.
- *Preconditions*: They list the requirements to be present in the system so the method is a successful way of attacking the system. Together with the "method" this list made up the "action" of the cyber-physical attack.
- *Influenced element*: It refers to the elements which have been manipulated through the described action.
- *Influence:* The produced changes in the influenced element. Together with the "influenced element", it describes the "cause" of the cyber-physical attack.
- Affected element: A list of the elements which have been affected by the changes in the system (usually it is the objective of the attack).
- Impact: A description of the changes in the system. Together with the "affected element", it describes the "effect" of the cyber-physical attack.

Considering the above descriptive language a functional architecture was proposed in [19] in order to provide a protection system for Industry 4.0 applications. It is shown in Figure 3 [19].

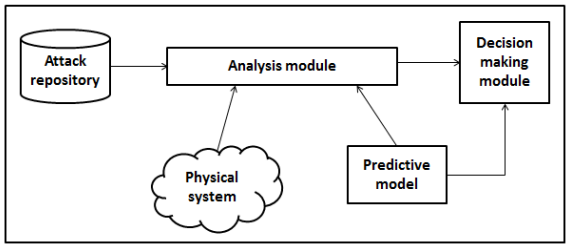

Figure 3: Functional Architecture [19]

In this architecture, different components may be identified. A predictive model represents the system's state in a certain moment and at some future instants. This model may be updated through a hybrid simulator and interpolation techniques. The information is provided to an analysis module, where the data is compared to the real state of the components in the system. Results of the comparison process are employed to infer if the system is under a cyber-physical attack.

The authors in [20] mentioned that security issues for smart products and digital manufacturing should be tackled in the design phase. They implemented a model using Hazard and Risk Assessment along with Threat and Risk Analysis (HARA and TARA). They use an example of an automotive electronic steering column lock system to use their method to incorporate functional safety and cyber-security in the early design phase.

IV. Process Models Using Existing Standards

The authors in [2] suggested a process model to assign security measures to vulnerabilities and threats of a system for Industry 4.0. This process model takes into consideration five main fields of requirements to address this issue. Diversity of systems and its processes (R1), defense in depth strategy (R2), threat analysis and risk assessment (R3), application specific security solutions (R4) and usability (R5). This is depicted in Figure 4 [2].

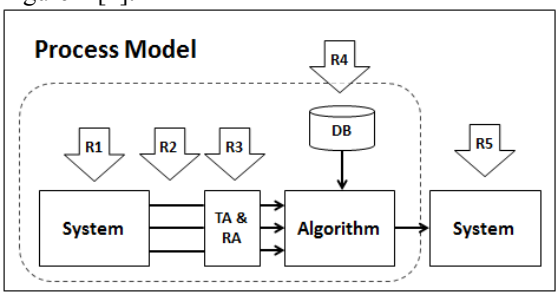

Figure 4: The Process Model that assigns security measures to vulnerabilities [2]

The above process model provides a simple model for SMEs that accepts an operational system as input and provides a semi-automated threat analysis and risk assessment. The results of this analysis are committed to an algorithm that semi automatically chooses adequate security recommendations to mitigate the risk and improve or eliminate the weaknesses of the current setup. This process model was based on the use of the standards IEC 61508 and IEC 62433. These standards consider the functional safety of safety-related electrical systems, electronic and programmable electronic systems as well as IT systems for ICSs. To further elaborate on them, each standard will be addressed individually. The IEC 61508 standard's main focus is to avoid personal injury; property damage reduction comes in second place. In the case of threats on functional safety that are related to IT security, the standard refers to IEC 62443 standard. The IEC 62443 is based on three IT security pillars, zones and conduits, threat analysis and security assessment and security levels. Zones can be explained as the physical or logical network segregation. Conduits can be translated into the communication that takes place across the communication channels.

The need of IT governance comes from the need of having the ability to measure and control compliance with widely agreed upon standards. The two main aspects of IT governance are

performance and conformance. Performance can be translated into the task of controlling or influencing the effectiveness of the company's operations to create enterprise value. Conformance, however, translates into the compliance of the enterprise with standards, regulatory requirements and legal constraints. IT governance plays the role of mitigating the IT risks caused by cyber-security threats. COBIT 5 framework is used to achieve IT governance. It breaks down enterprise goals into IT related goals; it also defines processes and associates them with certain activities to make sure that the goals are reached. The different types of COBIT 5 goals and processes may be used to access how the framework addresses the security challenges attributed with the up rise of Industry 4.0. Figure 5 [3] shows a conceptual model of IT governance with respect to COBIT 5 framework.

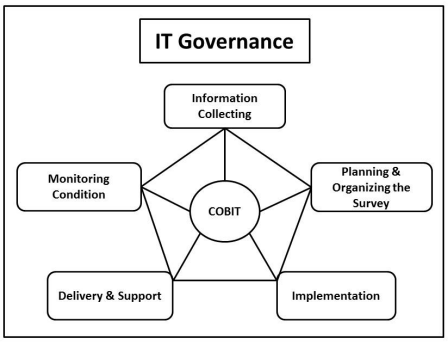

Figure 5: Conceptual IT Governance Model with respect to COBIT 5 [3]

V. Conclusions and Future Work

IT security in Industry 4.0 is accompanied by many challenges. The diversity of systems and components, as well as the increasing use of internet technologies in the production area, and the merger of cyber-physical production systems (CPPS) with IoT, make industrial plants vulnerable to several attack vectors and cyber-security attacks. RAMI 4.0 is the common reference point for any system modeling in Industry 4.0. In this paper, we touched upon several attack scenarios, as well as their impact on smart manufacturing. The mitigation techniques to use for these attacks, and the standards implemented that address the topic of security for the several components facilitating the emergence of Industry 4.0 were presented. This paper is merely to highlight all the above risk, repercussions and mitigation techniques to emphasize on the importance of having a robust guideline in each layer of the RAMI 4.0 standard addressing security by design. In order to securely design systems and mitigate all the disastrous outcomes of a cyber-security attack on any of its various components.

References

[1] Y. Wang, T. Towara and R. Anderl, "Topological Approach for Mapping Technologies in Reference Architectural Model Industrie 4.0 (RAMI 4.0)," *Proceedings of the World Congress on Engineering and Computer Science,* vol. 2, 2017.

[2] Y. Wang, O. Anokhin and R. Anderl, "Concept and Use Case driven Approach for Mapping IT Security Requirements on System Assets and Processes in Industrie 4.0," *Procedia CIRP 63.1, Elsevier,* pp. 207-212, 2017.

[3] M. Savtschenko, F. Schulte and S. Voß, "IT Governance for Cyber-Physical Systems: The case of Industry 4.0," *International Conference of Design, User Experience, and Usability. Springer, Cham,* pp. 667-676, 2017.

[4] T. Pereira, L. Barreto and A. Amaral, "Network and information security challenges within Industry 4.0 paradigm," *Elsevier,* vol. Procedia Manufacturing 13, pp. 1253 - 1260, 2017.

[5] A. Varghese and D. Tandur, "Wireless requirements and challenges in Industry 4.0," *International Conference on Contemporary Computing and Informatics (IC3I), 634,* 2014.

[6] T. Lins, M. Silva and R. Oliviera, "Proceedings of the 20th Advanced International Conference on Telecommunications. Valencia, Spain," pp. 34 - 39, 2016.

[7] R. Darth and A. Horch, *IEEE Ind. Electron. Mag. 8,* pp. 56 - 58, 2014.

[8] D. Ding, Q. Han, Y. Xiang, X. Ge and X. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Elsevier,* vol. Neurocomputing 275, 2018.

[9] M. Long, C. Wu and J. Hung, " Denial of service attacks on network-based control systems: Impact and mitigation," *IEEE Transactions on Industrial Informatics,* vol. 1, no. 2, pp. 85 - 96, 2005.

[10] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications,* vol. 11, no. 6, pp. 38-43, 2004.

[11] P. Lee, A. Clark, L. Bushnell and R. Poovendran, "A passivity framework for modeling and mitigating wormhole attacks on networked control systems," *IEEE Transactions on Automatic Control,* vol. 59, no. 12, pp. 3224-3237, 2014.

[12] D. Ding, Z. Wang, D. Ho and G. Wei, "Observer-based event-triggering consensus control for multi-agent systems with lossy sensors and cyber attacks," *IEEE Transactions on Cybernetics,* vol. 47, no. 8, pp. 1936-1947, 2017.

[13] P. Varga, S. Polsz, G. Soos and C. Hegedus, "Security threats and issues in automation IoT," *Factory Communication System (WFCS),* vol. 2017 IEEE 13th International Workshop on. IEEE, 2017.

[14] A. Sadeghi, C. Wachsmann and M. Waidner, "Security and privacy challenges in industrial internet of things," *Design Automation Conference (DAC),* vol. 2015 52nd ACM/EDAC/IEEE. IEEE, 2015.

[15] N. Benias and A. Markopoulos, "A review on the readiness level and cyber-security challenges in Industry 4.0," in *Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, South Eastern Europe. IEEE, 2017.

[16] A. Wegner, J. Graham and E. Ribble, "A New Approach to Cyberphysical Security in Industry 4.0," *Springer,* vol. Cybersecurity for Industry 4.0, 2017.

[17] R. Nair, C. Nayak, L. Watkins and K. Fairbanks, "The Resource Usage Viewpoint of Industrial Control System Security: An Inference-Based Intrusion Detection System," *Springer,* vol. Cybersecurity for Industry 4.0, 2017.

[18] J. Lopez, C. Alcaraz, J. Rodriguez and R. Roman, "Protecting Industry 4.0 against Advanced Persistent Threats," *Euro CIIP Newslett 11,* 2017.

[19] B. Bordel, R. Alcarria, D. Sanchez-de-Rivera and T. Robels, "Protecting Industry 4.0 Systems Against the Malicious Effects of Cyber-Physical Attacks," *Springer, Cham,* vol. International Conference on Ubiquitious Computing and Ambient Intelligence, pp. 161-171, 2017.

[20] A. Reil, C. Kreiner, G. Macher and R. Messnarz, "Integrated design for tackling safety and security challenges of smart products and digital manufacturing," *El sevier,* Vols. CIRP Annals-Manufacturing Technology, 2017.