The State of Cybersecurity in Smart Manufacturing Systems: A Systematic Review

Armando Araújo de Souza Junior, José Luiz de Souza Pio, Jó da Cunha Fonseca, Marcelo Albuquerque de Oliveira, Otávio Cesar de Paiva Valadares, and Pedro Henrique Souza da Silva

ABSTRACT

With the advent of the so-called 4th Industrial Revolution, personified in the globally commented Industry 4.0, there is a change in progress in manufacturing systems, provided by the development of communication and information technologies, adding an intelligence component in manufacturing plants, through the possibility connectivity and interaction throughout the production chain (intelligent manufacturing systems or cyber-physical systems). However, this new paradigm has an extremely sensitive component, which is the question of the security of the data that is transferred and of the production processes itself. Due to this premise, this article proposed to bring, through a systematic literature review, research about the academic works related to security in these new manufacturing structures (smart manufacturing systems), analyzing which strategies, methodologies, techniques, and technologies have currently used to learn about their vulnerabilities and mitigate possible attacks.

Keywords: cybersecurity, fourth industrial revolution, industry 4.0, security, smart manufacturing, smart manufacturing systems, systematic review.

I. INTRODUCTION

There is a new industrial revolution in progress (4th revolution), and different from the other (1st, 2nd and 3rd), appears to be more disruptive and with implications that go far beyond the limits of manufacturing plants. According to Schwab (2017), this revolution is characterized by changes never seen in history, compared to its speed, amplitude, and depth, bringing in its essence the fusion of technologies and the interaction between physical, digital, and biological domains.

In the wake of this revolution, the industrial manufacturing is undergoing a profound transformation. Due to the development of new communication and automation technologies and the business need to adapt to the new times, with cost reduction, flexibility and the development of new competitive capabilities, a new manufacturing concept emerged, the so-called Industry 4.0. The term was developed by three German engineers at the Hannover Fair in 2011 as a new political, industrial, and academic concept to revitalize German industry (Kagerman et al., 2011).

This new paradigm has spread throughout the world since then and is in process of construction, either by academia or the industry itself. As a consequence, traditional automation-based, computer-controlled industrial manufacturing systems are gradually and slowly being absorbed by Smart Manufacturing Systems - SMS’s (Tuptuk & Hailes, 2018). Such systems are one of the pillars of Industry 4.0 and their implementation is possible due to the digitalization of industrial processes and the connectivity between machines, virtual systems, and people (Hermann et al., 2016).

In this context of digitized and highly connected environment, several challenges arise, among which, the issue of data security and production operations, given the high risk of attack on these systems, and their vulnerabilities, which are not yet fully known (Tuptuk & Hailes, 2018).

Considering this obstacle, this paper was premised on conducting a systematic literature review on the scientific production related to security in these systems, analyzing which strategies, methodologies, techniques, and...
technologies have currently been used to mitigate attacks.

The paper is organized as follows: section one presents a concise introduction on the subject discussed and the purposes of this work; then, the theoretical framework unveils current scientific knowledge about industry 4.0, smart manufacturing and intelligent manufacturing systems; in section three the systematic review methodology is presented; section four presents the research results, with due discussions; finally in section five, the conclusion closes the work, listing possible future implications.

II. LITERATURE REVIEW

A. Smart Manufacturing

Technological development together with the ubiquity of the internet has allowed the digitalization of physical means, providing a connection between the real world and the virtual world (Schwab, 2017). Today, it is common for people to be connected with each other, through social networks, and instantly access various services (transport, online shopping, streaming etc.), through computers and smartphones (Schwab, 2017). Similarly, this digitization and connectivity has been incorporated by the manufacturing industry, adding intelligence to already automated factory floors. (Tuptuk & Hailes, 2018).

Intelligent manufacturing, advanced manufacturing, industry 4.0 and intelligent factory are concepts used in different countries (U.S, Germany, South Korea, Japan and so on), with similar meaning, to designate and/or define this new manufacture (Mittal et al., 2019). According to the pioneers of industry 4.0, this transformation imposes an almost complete break from the concepts and standards that have shaped industrial processes so far (Kagermann et al., 2013).

This remodeling is grounded, and here there is unanimity among academics, basically on two pillars – technological and conceptual, in which, depending on each approach and vision of the researcher/country, one or another technology is adopted, one or another concept is considered. However, despite these differences, there is a recurrent core of citations, both of enabling technologies and implementing concepts. In the case of technologies, there is the Internet of Things (IoT), Cyber-Physical Systems (CPS or CPPS), Cloud Computing, Big Data, Artificial Intelligence (AI) and 3D printing; within the concepts, interoperability, decentralization, modularity, virtualization and real-time response (Hermann et al., 2016; Kagermann et al., 2013; Kusiak, 2017; Mittal et al., 2019; Tuptuk & Hailes, 2018).

Therefore, a definition of smart manufacturing is still under construction and there is still no definitive concept fully accepted by the academic community and industry (Kusiak, 2017; Tuptuk & Hailes, 2018), however, the National Institute of Standards and Technology (NIST) of the United States captures the essence of this new manufacture: a fully integrated and collaborative manufacturing system that responds in real time to meet changing demands and conditions in the factory, the supply network and customer needs.

According to Kusiak (2017), smart manufacturing integrates legacy and future physical assets from the shop floor, through sensors, computing platforms, communication technology, intensive data modeling, control, simulation, and predictive engineering, using the concepts of systems physical – cybernetics (CPS), internet of things and everything (IoT, IoE), cloud computing, service-oriented computing (IoS), artificial intelligence (AI) and data science.

Considering this definition, Kusiak (2017) proposed a general architecture, as illustrated in Fig. 1, with two basic layers, one corresponding to the shop floor equipment and the other cybernetic, connected by an interface, where the manufacturing equipment would have its own intelligence, leaving to the cybernetic layer the intelligence of the whole system.

Understanding this new architecture requires an understanding of how today's manufacturing is still structured, as it absorbs part of the technologies that developed with the advent of the so-called third industrial revolution, in this case, automation and computing.

This manufacturing model is composed of five layers or levels, according to Tuptuk & Hailes (2018). Level 1 – acting (sensor, actuator, data acquisition); level 2 – cell control (PLC, robots); level 3 – production supervision (SCADA, database); level 4 – production management (MES); and level 5 – corporate management (ERP). The Fig. 2 presents this hierarchical structure, showing the layered levels of computer systems and communication connections that are commonly used in this architecture (computer-integrated manufacturing model - CIM) (Tuptuk & Hailes, 2018). It is a rigid and centralized structure, in contrast to intelligent manufacturing that proposes a flexible and decentralized architecture, in which the elements of the conventional model (CIM) are aware of their environment and autonomous, interacting with each other and capturing data to generate information (Tuptuk & Hailes, 2018).

![Fig. 1. General architecture of a smart factory. Source: adapted from Kusiak (2017).](image)

These authors also stated that within the scope of this vision, decision-making will be decentralized and processed in real time, as the system components will have attributes such as self-governance, self-organization, self-awareness, self-maintenance, and self-repair.
In this way, there is a new structural idea, now constituted by physical-cybernetic systems that would interconnect all “actors” of the internal “ecosystem” (machines, production processes, workers, managers) and external of production (suppliers, customers, etc.), thus allowing their interactions (Kagermann et al., 2013).

B. Smart Manufacturing Systems

As there is not yet a very clear and uniform definition of the concepts of smart manufacturing systems - SMS, they get confused with physical-cybernetic systems and with the very framework of smart manufacturing, often being treated as synonyms (Liu & Jiang, 2016; Zheng et al., 2018). However, Qu et al. (2018), trying to situate the smart manufacturing systems - SMS, proposed a conceptualization molded in three points of view:

- **Engineering** – whereas intelligent manufacturing would be an intensified application of advanced intelligent systems to enable rapid manufacturing of new products, dynamic response to demand and real-time optimization of production and supply chain networks, SMS would be the new platforms that would integrate these systems in a rich learning environment.

- **Interconnection and Communication** – using sensors and communication technology to capture data at all stages of manufacturing, SMS would be gaining intelligence, increasing production rate and reducing waste and errors.

- **Precise decision** – SMS based on Big Data would optimize the planning and control of manufacturing operations.

Still according to these authors, smart manufacturing systems (SMS) obtain real-time data, improving decision-making accuracy, increasing industrial plant efficiency and performance, thus increasing overall productivity. In comparison, cyber-physical systems (CPS) are collaborative computational entities that integrate the physical and virtual systems of smart factories, simultaneously providing and using data and data processing available in cyberspace, to provide the attributes of decentralization, interoperability, control and real-time response in production processes (Liu & Jiang, 2016; Monostori, 2014).

According to Monostori (2014), cyber-physical production systems (CPPS) are made up of autonomous cooperative elements and subsystems that connect to each other, depending on the situation required, at all levels of production, from processes performed by machines to networks production and logistics.

Therefore, the hierarchical model of production system paradigm is replaced by the distributed service prototype, as shown in Fig. 3, transforming the intelligent manufacturing ecosystem into a fully connected and integrated complex, in which all manufacturing functions along the three dimensions (product, production system, business) in the manufacturing pyramid can be virtualized and hosted as services, except for those time-critical and safety-essential manufacturing functions (Lu & Morris, 2016).

For Tuptuk & Hailes (2018), this new production set, highly connected and interactive with several other subsystems and multiple actors, becomes very vulnerable, as part of the security issues are being neglected and the designed architectures absorb IT and communication implementations extremely problematic. Considering that it would not be enough to protect manufacturing systems through isolation based on physical access control, since almost everything would be digitized and networked, it is essential to model an SMS with cybersecurity as the main point to be observed.

![Computer-integrated manufacturing (CIM) hierarchical model](image)

**Fig. 2.** Computer-integrated manufacturing (CIM) hierarchical model. Source: adapted from Tuptuk and Hailes (2018).

![Decomposition of the hierarchical modeling model by a service-based distributed system](image)

**Fig. 3.** Decomposition of the hierarchical modeling model by a service-based distributed system. Source: Monostori (2014).

### III. RESEARCH METHODS

This work adopted the methodology of application of systematic review proposed by Tranfield et al. (2003), in which, in the planning phase of the review, it was verified that cybersecurity is an issue that has permeated the concerns of global society, considering the cases alarming of confidential data leaks and attacks on IT systems around the world, therefore, it was verified the need to verify how this subject is being treated in the academic world, when considering the new Smart Manufacturing Systems – SMS. Therefore, an analysis of “the state of the art” was proposed.

The development of the systematic review took place according to the stages described in Fig. 4 (Tranfield et al., 2003).

In the preparation phase of the systematic review protocol, the following general research criteria were adopted:

- a. Search databases – CAPES/MEC journal portal (content available to the academic community), Google Scholar and Scopus;
- b. Keywords – “security”, “smart manufacturing systems”
and “cybersecurity”. Used in conjunction with the boolean operator AND;
c. Search criteria in the CAPES/MEC database – use of words security AND “smart manufacturing systems”, cybersecurity AND “smart manufacturing systems”. Refining: peer-reviewed journals, only articles, English language, from the engineering field and published between 2015 and 2021;
d. Search criteria in Google Scholar and Scopus database – use of words “security” AND “smart manufacturing systems”, “cybersecurity” AND “smart manufacturing systems”. Refining: only papers published between 2015 and 2021, in English, excluding patents and citations;
e. Criteria for inclusion of papers – developed subject aligned, in some way and with median depth onwards, to the presented theme;
f. Criteria for exclusion of papers – texts that addressed intelligent manufacturing systems, without considering the issue of cyber security.

In the second phase of conducting the research, the survey process in the databases took place between the months of march and april 2021. In the selection process, after the use of keywords and filters, the first selection criteria of the works were the verification that the title and abstract had some relationship with the topic to be researched. Afterwards, a complete reading of all selected articles was carried out, to choose the definitive articles. This entire process is described according to Fig. 5.

### IV. RESULTS AND DISCUSSIONS

After the surveys, 22 works were chosen that fit the proposed theme and the research objectives, as shown in Table I.

Safety issues in Smart Manufacturing Systems – SMS primarily involve a structural-functional problem, considering that the current production line comprises legacy equipment and advanced technologies, which are added day after day to the plant, by necessity or natural evolution, without considering their structural and functional security differences, thus imposing little-known vulnerabilities, which can be exploited in the future by people, groups, or nations with specific purposes (Tuptuk & Hailes, 2018). In this sense, Horak et al. (2021) reinforced that the concern with safety ends up being relegated to the background, precisely because of the very nature of manufacturing, which imposes a race for higher yields and productivity, where any stop for a restructuring would be equivalent to the loss of resources. However, the massive implementation of SMS, without first having the knowledge and correction of their vulnerabilities, could bring incalculable damage to the industry and even impact on national security issues for a country (Tuptuk & Hailes, 2018). Therefore, there is a need to consider security, thinking first about the architecture and then about the functionality, to detect the vulnerabilities of each constituent part of the system, proposing measures a priori.
To present potential challenges and threats regarding IoT applications and service domains.

To present the new challenges of cybersecurity in IIoT networks, as well as threats to security and protection risk perspectives, applying systems thinking to describe a diagrammatic and concrete view of Cyber-physical Systems, in addition to those presented in IEC 62351.

To present detailed analysis of security threats, possible attacks and security incidents, objectives and threats. In addition to analyze the impact of Cyber-threats on the performance of a smart manufacturing system.

Propose a method and conceptual framework for integrated functional safety analysis described in the generic standard for functional safety IEC 61508-x and cybersecurity of industrial systems.

To develop a theoretical basis for the principles and properties of intelligent manufacturing systems and reliability mechanism.

To explain how cybersecurity can impact Total Productive Maintenance affecting Overall Equipment Effectiveness (OEE) in a smart manufacturing system.

Elaboration of a multilayer graphic model generated by synthetic data with attack simulations, estimating power consumption, measuring the results, in addition to presenting a method for detecting anomalous events.

Provide a comprehensive security analysis of cyber-physical systems, with particular emphasis on CPES applications. In addition to a bibliographic review on the subject and a case study of attack and adversary models.

To discuss how blockchain systems can overcome potential cybersecurity barriers to gain intelligence in Industry 4.0. Reveal how cybersecurity issues are being identified by manufacturing systems.

Present detailed analysis of security threats, possible attacks and security requirements based on standards and norms to protect IEC 61850 power system communications, in addition to those presented in IEC 62351. Provide insight into SCADA communication architecture and protocols, which are used in diverse industrial applications transport, telecommunications, power generation and manufacturing industries. Discuss high-impact security incidents, objectives and threats.

Examine the main characteristics of CPS and its relationship to other types of systems, defining their dependencies between levels of automation and human functions from a systems engineering perspective, applying systems thinking to describe a diagrammatic and multilayered representation of CPS for analysis combined security, protection risk.

To present the new challenges of cybersecurity in IoT networks, as well as the known practices for mitigating adversities. In addition to analyze the result of point-to-point intelligent network routing based on "garlic" routing as a proposal for modeling secure network communications in the field of IoT.
Dimensioning security issues in SMIs is of paramount importance, as the potential result of an attack on these systems could range from simple economic losses to loss of life, with impacts on the entire production and value chain (Tuptuk & Hailes, 2018). Therefore, it is essential to know their vulnerabilities, however, there is little understanding about them, as SMS are still in their infancy and, consequently, the possible attacks are not recognized. However, some researches have proposed some theoretical and practical approaches to fill this gap.

The confrontation of these security problems in SMS involves the approach of two great dimensions – the physical and the logical which can be analyzed together or separately, with propositions of practical or conceptual applications. Horak et al. (2021), Huraj et al. (2021) and Wu et al. (2020), proposed, respectively, a practical investigation of attacks on real production lines with an emphasis on the Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices to prove their weaknesses; creating a communication map and preventing communication degradation from infected IoT devices at the switch level towards the production line; use of machine learning to detect and prevent intrusions; and a testbed to investigate cyber intrusions, validating countermeasures. Already Bracho et al. (2018), Leander et al. (2020), Kosmowski et al. (2019), Kühnle et al. (2017), Lopez et al. (2017) and Zarreh et al. (2019), designed a more conceptual analysis of security issues through statistical testing; formulating a list of access control requirements for an intelligent manufacturing system; use of risk charts to determine and verify the level of performance and integrity of security functions; categorization of anomalies and detection mechanisms; and unification into a common framework to help identify potential solutions.

From the point of view of computational and logic issues, Dakhnovich et al. (2018), Tedeschi et al. (2019) and Liu et al. (2020), proposed applying garlic routing to ensure the secure integration of segments into a digital manufacturing enterprise network; protecting sensitive data on the industrial internet based on local storage, fog and cloud; and an IoT endpoint security design.

In “analysis of threats to information security in digital production networks”, Dakhnovich et al. (2018), when describing digital production systems (another name for SMS), listing the main security implications involved in this new model (information flow), proposed an approach for building a security control system based on three principles: prevention, stability and zero confidence. Such a developed system should remove vulnerabilities and their sources, detect, and prevent object-oriented attacks and simulate the attacks and conditions of the digital production system, at three levels: operational, tactical, and strategic.

V. CONCLUSION

Considering that manufacturing systems have become increasingly dependent on data transfer, information and communication technologies, and that being connected is fundamental for the modeling of an SMS, with cybersecurity as its main point. A bibliographical review was carried out, with the objective of identifying researches and solutions used to analyze which strategies, methodologies, techniques and technologies are currently being used, as well as knowing the vulnerabilities and mitigating possible malicious attacks.

With the need for constant connectivity and recent technological advances and with the fact that SMS has become increasingly intertwined with communication protocols that circulate in networks, it was observed that such systems are more exposed and vulnerable to malicious attacks. In this context, much has been studied in order to understand vulnerability and its impacts, identify the means of propagation, in addition to bringing to light situations and case studies for exploitation.

Thus, by not having the appropriate level of security in their networks, from a security perspective, many industries have become targets of malicious attacks, which exploit unmapped vulnerabilities and can manipulate values, perform unforeseen actions or even collapse, compromise and paralyze an entire system.

In this context, it was observed that SMS security is associated with the guidance of cybersecurity practices from the design or modeling phase, adopting techniques and methodologies for protection, security, and mitigation of possible attacks. As technologies evolve, it is necessary to reassess the system to map new vulnerabilities.

However, what is observed is that as the benefits of Industry 4.0 and SMS are explored, so are new challenges in acquiring the safest means to develop them. In this sense, through the study and investigation of malicious attacks and the identification of risks, countermeasures for future attacks are developed. It can also associate with the use of machine learning and artificial intelligence the development of even better tools.

As a suggestion for future work, there is the study of protocols that make access difficult, processes that map vulnerabilities, as well as new technologies and advances in cybersecurity. Also fitting the analysis of projects for safer and more resilient systems.

REFERENCES


A cyber


