IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 20, 2021, accepted January 27, 2021, date of publication February 3, 2021, date of current version February 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3056650

A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0

VALENTIN MULLET, PATRICK SONDI, AND ERIC RAMAT
Université Littoral Côte d'Opale, F-62228 Calais, France

Corresponding author: Valentin Mullet (valentin.mullet@univ-littoral.fr)

This work was supported in part by the CPER ELSAT2020 project, in part by the French State, and Industry of the Future Program, both by the European Union with the European Regional Development Fund, and in part by the Hauts-de-France Region Council.

ABSTRACT Industry 4.0 is a revolution in manufacturing by introducing disruptive technologies such as Internet of Things (IoT) and cloud-computing into the heart of the factory. The resulting increased automation and the improved production synergy between stocks, supply chains and customer demands, come along with the threats and attacks from the Internet. Despite extensive literature on the cybersecurity topic, many actors in manufacturing factories are just realizing the impact of cybersecurity in the preservation of their business. This paper introduces step-by-step the concepts and practical aspects of an Industry 4.0 manufacturing factory that are related to cybersecurity. Based on a subdivision of a typical factory into several generic perimeters, we present the vulnerabilities and threats regarding the network and devices usually found in each perimeter. Therefore, it is more efficient to present the recent proposals of the literature regarding cybersecurity guidelines and solutions in Industry 4.0. Instead of spreading a lot of references regarding every aspect of cybersecurity, we focused on a limited number of papers among the recent references. However, for each paper, we provide the details about the purpose of the proposal, the methodology adopted, the technical solution developed and its evaluation by the authors. These solutions range from classical cybersecurity countermeasures to innovative ones, such as those based on honeypots and digital twins. In order to deliver a review also useful to non scientists, we present our guidelines along with those of some organizations involved in cybersecurity harmonization and standardization in the world.

INDEX TERMS Cybersecurity, intelligent manufacturing systems, Industrial Internet of Things, industrial control system, cyber-physical systems, manufacturing execution systems.

I. INTRODUCTION

The industrial sector has gone through several revolutions. Mechanization was the first stage. Then came mass production and electricity in a second step. The third one occurred in the 1970s with the introduction of automation and IT equipment bringing digital technologies into factories.

In 2011, the German government defined the concept which would represent the fourth step in the evolution [1] of traditional factories to make them more flexible and more adapted to ever-changing production environments: the Industry 4.0 paradigm, also known as Industrial Internet of Things [2] or Industrial Internet (see figure 1). Technically, Industry 4.0 aims to connect agricultural holdings and manufacturing factories to the Internet, in order to improve their efficiency and productivity (about 15% to 20%). This hyper-connectivity will allow the gathering of a high volume of data from the value chain for multiple uses such as:

- information exchange between the devices belonging to factories, suppliers or clients;
- data acquisition and storage for both traceability and digital performance management;
- data processing for predictive maintenance or remote monitoring, in order to reduce machine downtime;
- automation and reduction of inventories;
- improvement of both service levels and product quality.

To create this smart production environment, disruptive technologies will be required to handle autonomous communications between all industrial devices throughout the factory and the Internet. These technologies [3] include Internet of Things (IoT), cloud computing, big data, digital twin, augmented reality, 3D printing, artificial intelligence, new

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

generation Cyber-Physical systems (CPS). In addition, Industry 4.0 encourages the application of these technologies to enable distributed communication architectures (P2P-like), instead of relying only on typical cloud or other centralized architectures [4].

The integration of this heterogeneous equipment into the industrial cyber environment makes cybersecurity considerations mandatory in the design strategy of the companies that seek to embrace the Industry 4.0 paradigm. Despite the improvement brought by Industry 4.0 in manufacturing factory efficiency, cybersecurity breaches would involve critical impacts on the business model and loss of competitiveness [5]. Further description of Industry 4.0 concepts and applications is proposed in [6], as well as some recent cybersecurity attacks observed in several manufacturing factories in the world. The authors also propose countermeasures to face a wide range of cybersecurity risks. Another survey proposed in [7] focuses on cybersecurity. The authors particularly analyse the shift of an Industrial Control System (ICS) from a stand-alone plant to a cloud-based environment, while focusing on machine learning solutions. Among the most recent surveys, [8] also investigated machine learning solutions for tackling faults in the Industry 4.0 era. However, their study does not specifically address cybersecurity. A more specific recent survey [9] reviewed 262 papers regarding every aspect of Industry 4.0 security. Besides a systematic review of the literature, their main proposals focus on the opportunities brought by Fog computing in this field. All these references are classical surveys that aim at providing a complete view of the literature to the reader.

However, other surveys show that only 16% of companies are ready to face cybersecurity challenges [10]. Among the given reasons there is the lack of accurate reference standards, and the lack of managerial and technical skills to understand and implement them. Several organisations working on guidelines and standards help the companies to understand which scheme they should use in order to reinforce their security, and make it compliant. Among these organisations, to mention a few, we can find (please refer to appendix for acronyms): ANSSI (in France), ENISA (in the European Union), and NIST (in the United States of America). Therefore, instead of spreading a lot of references regarding every aspect of cybersecurity, in this work we decided to focus only on a limited number of papers among the recent references. However, for each paper, we provide the details about the purpose of the proposal, the methodology adopted, the technical solution developed and its evaluation by the authors. In this way, we hope that it will be useful to scientists as well as to compagnies in order to integrate the last trends regarding cybersecurity in their research and development work. The title of this paper refers to three themes, which are Industry 4.0, cybersecurity and manufacturing factory. After a brief overview of the Industry 4.0 concept in this section, summarized through figure 1, the remaining of this paper will focus on cybersecurity solutions and guidelines for

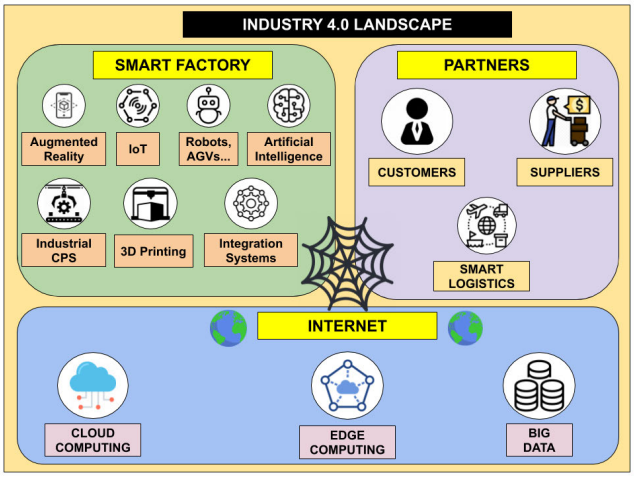

FIGURE 1. Industry 4.0 landscape with main technologies.

manufacturing factories in industry 4.0. To that end, a complete overview of the cybersecurity topic in the industrial context is needed to grasp the real stakes of the related issues.

In section II, a characterization of cybersecurity in Industry 4.0 regarding technical and managerial aspects is proposed. The goal is to become familiar with the concept, understand the implications, the impacts and the challenges for all entities involved. The overall organisation of this paper follows the structure depicted in figure 2. The factory is divided into several perimeters based on cybersecurity considerations in section III. For every perimeter, the specific equipment, monitoring systems, access control techniques and communication network solutions available through the literature are reported. The vulnerabilities, threats, risks and business impacts related to cybersecurity for Industry 4.0 are investigated in section IV. The threats will be detailed, along with the appropriate terminology, according to the factory perimeters involved. In addition, the business

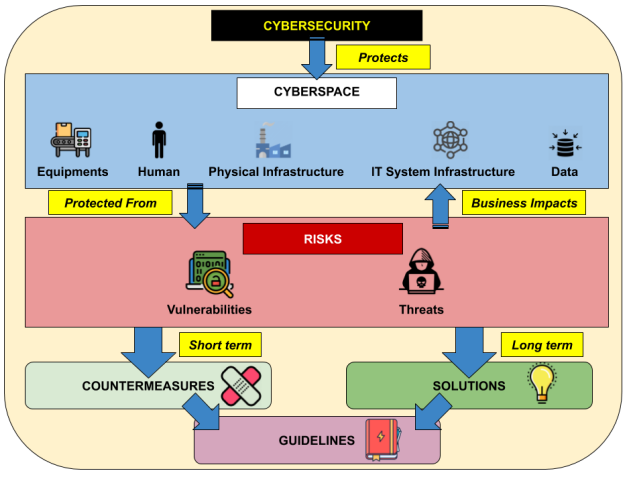

FIGURE 2. Cybersecurity technical characterization.

impacts are addressed in order to highlight the relation with real-world situations. Section V presents the countermeasures to cyberattacks against factories, and cybersecurity solutions for Industry 4.0 found in the literature. For each selected solution, the purpose of the solution, the related methodology and its implementation will be detailed. A comprehensive review is proposed to point out the accuracy of each solution. Finally, section VI proposes our guidelines to cybersecurity solution implementation in factories, resulting from this review of the literature, before the conclusion of the paper.

II. CYBERSECURITY CHARACTERIZATION

Cybersecurity is often associated with two famous stereotypes, which are ''The subject is only technical'' and ''The subject is reserved for the IT domain''. The first objective will be to show that the concept actually goes beyond these ideas. To that end, this section will characterize cybersecurity on both technical and managerial aspects.

A. TECHNICAL CHARACTERIZATION

A characterization of cybersecurity is proposed in Fig.2, and tries to answer the following questions inspired from [10]:

- Who/What is involved and should be protected?
- What should they be protected from?
- How to protect them?

1) WHO/WHAT?

The global perimeter covered by cybersecurity is called ''cyberspace''. Inside this space, can be found every actor who has any form of interaction with the system, which includes:

- Equipment (machines, devices, mobile, etc. . .);
- Humans (users, administrators, visitors. . .);
- Physical infrastructure (building, factory, companies);
- IT infrastructure (networks, applications, processes);
- Data generated by all these actors.

The cyberspace is not restricted to a virtual world, and is actually involved in the concrete physical world.

2) FROM WHAT?

The cyberspace defined above must be protected from different risks such as those due to intrinsic vulnerabilities or those raised by attacks performed by cybercriminals. When cybersecurity measures are not able to prevent those risks, they have consequences in the physical world. In the context of manufacturing, those consequences are called ''business impacts'', and they will be also investigated in this paper.

3) HOW?

To deal with those risks, cybersecurity can deploy the following two types of protection: countermeasures which are usually dedicated to immediate and short term usage, and long term prevention and protection solutions. Relying on these concepts, it is possible to establish guidelines for an efficient and protective cybersecurity solution.

B. MANAGERIAL CHARACTERIZATION

This management view of cybersecurity developed in [11] completes the technical one. The related illustration is depicted in figure 3. Industry 4.0 relies considerably on information systems and technologies, which raise cybersecurity as a top priority. However, due to complexity of the related issues, there is often a confusion about the necessary actions. In addition, cybersecurity professionals often fail to make these actions accessible to non-technical stakeholders. The vision of cybersecurity management relies on three notions, which are: strategy definition, strategic aspect with value creation and awareness of cybersecurity importance.

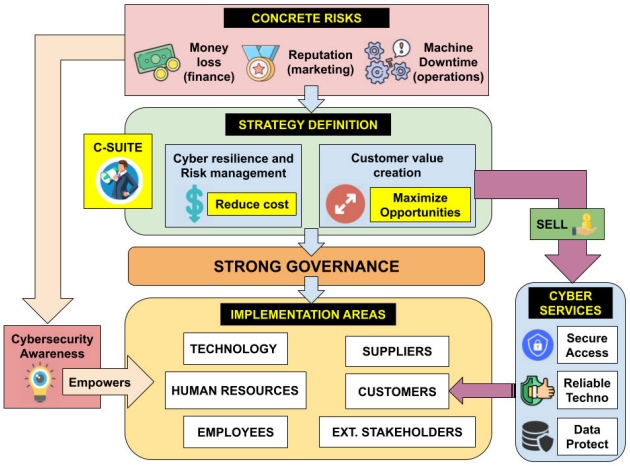

FIGURE 3. Cybersecurity managerial view.

1) STRATEGY DEFINITION

From an IT perspective, when communicating about cybersecurity, the common issues are usually:

- a reactive approach: the subject is important only after a major crisis;
- oversimplification: IT vendors spread the idea that the amount spent determines the degree of protection;
- lack of interest: cybersecurity is seen as pure cost, without guaranteed benefits.

In order to overcome these issues, the first step should be to consider cybersecurity management as part of a strategy definition, and not just as a protection solution. To justify the need of this strategy, it should be presented as a response to concrete cybersecurity risks, which are easier to understand by non-technical people: financial loss for the Finance department, bad reputation for Marketing department and machine downtime for Production operations, etc. The Managers start to approach the issue through cyber resilience and risk management in order to minimize the cost related to uncertainty, and to ensure the continuity of business operations. Then, the customers must be integrated into this definition through customer value creation. The involvement of corporate leaders, chief suite (C-Suite) and cross-functional collaboration is essential to complete this step. Moreover, to apply this strategy, a strong governance must be established to ensure

that it will be respected in implementation areas. This is generally defined through an Information System Security Policy (ISSP).

2) STRATEGIC ASPECT

The companies handling customer data may now consider cybersecurity as an opportunity to develop smart products and create customer value. They can sell various cyberservices to the customer such as secure access, reliable technology, and data protection. These services are opportunities for companies to get new sources of additional revenue, and customer willingness to pay for these ''premium services'' could be stimulated by using trust as a critical argument in the commercial interactions with them.

3) AWARENESS

Awareness consists in spreading the idea that cybersecurity involves everyone in order to empower people. This process takes place in implementation areas where cybersecurity strategy is applied.

These areas are not always clearly mentioned, and sometimes even forgotten. Our management characterization of cybersecurity considers the following areas:

- Technology: every technical area, often falsely considered as the only one concerned by cybersecurity;
- Human resources and employees: as the root of successful cyberattacks, which are often due to employee negligence, malicious behaviour or process failure;
- Direct and multi-tier partners that feed various threats;
- Customers and external stakeholders.

Human resources departments need to develop competencies and capabilities because most organisations are characterized by low employee awareness and basic cybersecurity knowledge. Their role is even more critical to achieve overall awareness, since they have the most direct contact with all the employees of a company. With regard to customers and stakeholders, companies try to make them aware of cybersecurity importance, but the latter experience a low willingness from the previous to pay for additional product features or services. Some companies plan to pilot new tools for assessing and communicating about cyber-risks to obtain customer engagement in this domain. An interesting concrete study regarding these aspects is presented in [12].

III. CYBERSECURITY PERIMETERS IN A FACTORY

In order to understand cybersecurity in an industrial environment, it is important to remember that the factory contains several departments with different needs and working processes. We first propose a subdivision of the factory into six generic areas that we call theperimeters.

A. DEFINITIONS AND EQUIPMENT

1) MANUFACTURING-PRODUCTION

This is the main area in a factory where the production lines are located, each one dedicated to some of the many steps needed to manufacture the final products. The devices found in this perimeter belong to two groups: ICS (Industrial Control System) and CPS (Cyber Physical System). ICS mostly gathers the control components, which act together to achieve an industrial objective [10].

They have been used since the second half of the 20^{th} century [13]. Inside this category, can be mentioned PLC (Programmable Logic Controllers), RTU (Remote Terminal Units) [14], IED (Intelligent Electronic Devices). To interact with the hardware controller and get the data gathered by the ICS environment, the administrators have a Human Machine Interface (HMI), which is also used to display the devices status [15].

CPS are related to anything that integrates computation, networking or physical processes. They allow interaction between the digital world and the physical one. As an example, a manufacturing line can be considered a CPS [10]. Indeed, they use sensors and other embedded systems to collect data from physical processes. Several authors [10], [16], show that ICS is an application area of the CPS.

2) LOGISTICS

Industrial logistics is different from the traditional one, due to its adaptation to handling production flow, thus making its action area wider. Its perimeter is made up of multiple structures such as workshops and warehouses where forklifts are used. In this area where mobility is a key point, wireless devices are mostly used (bar code scanners, tablets).

3) ACTIVE SUPERVISION

The active supervision represents the tertiary activity, which covers the office part of the factory. It groups together departments such as accounting, sales, human resources (HR), local IS, etc. The most common devices are desktop computers, smartphones, screens, printers, etc.

4) RESEARCH AND DEVELOPMENT

Research and development refers to laboratories and offices related to innovation, and developing new products or services. This is the first step of the development process, which means that some equipment is new or experimental. The engineers use devices that are more powerful than common desktop computers, and usually require specific setup.

5) LIVING AREA

The living area matches with the places where the employees gather (canteen, meetings rooms, rest rooms, etc.). In these areas, can be found VoIP phone, tablets, displays, etc.

6) EXTERNAL AREAS

The external area refers to everything outside the factory plant. It includes the physical places such as parking, as well as virtual places like the Internet (cloud, etc.).

B. INTERACTIONS BETWEEN PERIMETERS

The perimeters play a role in the manufacturing process, and their interaction at the IS level is mandatory (Table 1).

TABLE 1. IS interactions (X) between factory perimeters.

	Presence of IS interactions					
	MAN	LOG	SUP	RD	LIV	EXT
MAN	X	X	X	X		
LOG	X	X	X			
SUP	X	X	X	X	X	X
RD	X		X	X		
LIV			X		X	X
EXT			X		X	X

C. ACCESS CONTROL

Once there are interactions between perimeters, it is necessary to perform accurate access controls according to the information exchanged, which can be very sensitive. Table 2 shows the different kind of access controls available in the literature for the defined perimeters.

D. MONITORING

Another important aspect of security is monitoring, which allows users to be notified when a security breach appears, or when the system is under an attack. Table 2 describes some monitoring solutions applicable to manufacturing factories.

E. NETWORK ACCESS

One more aspect regarding the perimeters concerns their organisation regarding the network access. The most representative network solutions are summarized in table 2, and some of them are detailed in the following sections.

1) MANUFACTURING-PRODUCTION PERIMETER NETWORKS

In the manufacturing area, there are several types of ICS (Industrial control systems) [15]. These ICS are categorized in two layers: the physical control layer and the logical control layer. Three sub-networks exist in this perimeter: SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control Systems) and PLC / Sensors / Protocols. Figure 4 shows these different networks with the equipment and the communication protocols used.

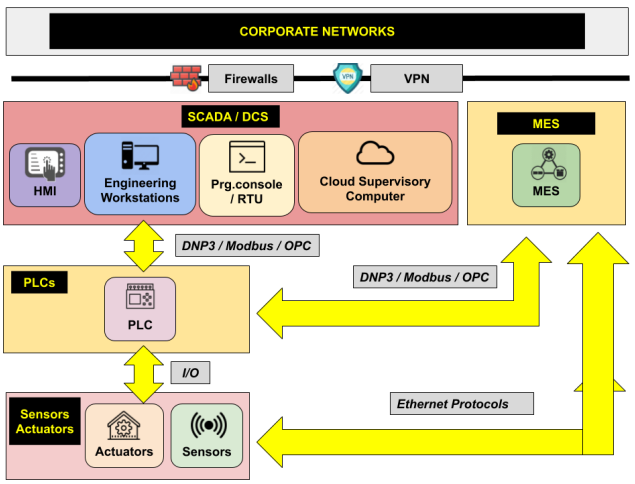

FIGURE 4. ICS networks overview.

a: SCADA

The SCADA allows supervision of data acquisition and monitoring of the production system. It is also used for remote control of the sites by the administrators adopting a centralized control system.

b: DCS

A DCS is made up of autonomous controllers installed across a manufacturing or a production unit. The DCS system uses these controllers to supervise and monitor a unit remotely. The difference between DCS and SCADA is that the SCADA can manage systems at multiple locations, contrary to DCS which is restricted to a single location.

c: PLC/SENSORS/PROTOCOLS

All control devices such as PLC (Programmable Logic Controllers), sensors or protocols (Distributed Network Protocols DNP3 / Modbus) can be found in this last sub-network, which is part of the physical control layer.

A PLC is the logic interface between SCADA and DCS systems. The PLC is supposed to receive control commands and return the status of the sensors. To establish the connection between PLC and SCADA, specific protocol communications have been designed by ICS suppliers.

One of these protocols is the DNP3, notably used in electricity and water treatment plants. Furthermore, the transmission of data between PLC and SCADA/DCS is ensured by the Modbus-TCP protocol, which uses TCP/IP and a serial communication channel.

2) THE OTHER PERIMETER NETWORKS

In this paper, we focus on manufacturing factories. Therefore, the other perimeters that can also be found in other organisational systems are not investigated further regarding network access. Usually, local area network (LAN) or wireless LAN are used for the internal perimeters, while Internet access is used for the others.

Some interesting references investigate network communication in Industry 4.0 [17], and more specifically regarding wireless communications [18], [19]. The general considerations regarding cybersecurity for the contexts where similar network access solutions are used, apply to these perimeters. Particular attention should be given to the interactions, at the network access level, between these other perimeters and the manufacturing perimeter.

IV. FACTORY VULNERABILITIES, RISKS, THREATS AND BUSINESS IMPACTS

Industry 4.0 factories have security vulnerabilities, like most organisational systems. The interconnection between the equipment makes security more complex, and brings unexpected vulnerabilities [20], [21]. In the industrial sector, manufacturing is the most targeted by security attacks, and the number of threats increases every year [10]. The first part of

TABLE 2. Factory perimeters in Industry 4.0.

	Equipment	Access methods	Monitoring methods	Networks
Manufacturing-Production	Industrial control system (PLC, RTU, IED, HMI)	login/password or access badge (human), device authentication through public & private keys (machines)	Video monitoring, traceability checks, logging, remote monitoring (SNMP or built-in)	PLC, DCS, SCADA
Logistics	Mobile terminals (tablet, bar code scanner, laptop)	access badge or access code (human), public/private keys or built-in (machines)	Video monitoring, information system checks, logging, remote monitoring (IDS/IPS probes)	LOG
Supervision	Desktops, printers, laptops, smartphones	login/password, access badge (for human), network and system checks (for devices)	system checks, logging, remote monitoring (SNMP)	Office
Research and development	Workstations, experimental devices	access badge or biometry (for human), network and system checks (for devices)	system checks, logging, remote monitoring (SNMP)	LAB
Living area	VoIP Phones, wireless displays, tablets	No specific access control for human, network and system checks for devices	video monitoring, remote monitoring (SNMP or built-in)	Office
External physical	Camera	access badge (human), network/system checks (devices)	Logging, video monitoring, remote monitoring (SNMP, etc.)	CAM
External virtual	Cloud providers	login/password (human), system & firewall rules (devices)	logging, traffic monitoring, IDS/IPS probes	Internet

this section will focus on the definition and the description of vulnerabilities, threats and risks.

A. DEFINITIONS

1) VULNERABILITIES

In the IT domain, vulnerabilities are defined by [10] as weaknesses that might be exploited by hackers to compromise the system. More precisely, these weaknesses can be either in the system, the security procedures or the internal controls. They can be classified into three categories, which are: remote access vulnerabilities, software vulnerabilities and LAN (Local area network) or WLAN (Wireless LAN) vulnerabilities.

2) THREATS

A cybersecurity threat (shortened to cyber threat) is defined by [10] as any circumstance impacting organisational operations, assets, individuals, other organisations or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information. Multiple parameters must be considered to analyse a cyber threat:

- The attack source (inside / outside);
- The objective;
- The cyber layer, including the execution layer (sensors, actuators), data transport layer (network) and application layer (user data storage).

In the context of Industry 4.0, the following main categories of cyber threats were identified [10], to mention a few:

- Direct attacks on external accesses;
- Indirect attacks with a service provider on which external access was granted;
- Unknown attack vectors (or zero-day exploits);
- Malicious softwares;
- Intrusion into neighbouring networks.

3) RISKS

According to [10], a risk is the level of impact on organisational operations, assets or individuals resulting from the potential impact of a threat and its probability of occurrence. In cybersecurity, risks are identified through the loss of some characteristics, which are availability, integrity, confidentiality and authentication.

a: AVAILABILITY

The attacks targeting availability intend to make the system unable to perform its usual tasks by overloading it. Their target can be the equipment or the related network access by disrupting it. The most common types are DDoS (Distributed Denial of Service) attacks, which try to flood the bandwidth or other resources of the system, making it unable to react. Some attacks also affect the network, and more precisely routing operations (grey hole, black hole, relay attacks).

b: INTEGRITY

Integrity consists in maintaining the accuracy and completeness of data. The related threats are similar to sabotage. They aim at altering the industrial communication protocols or the network traffic. One important issue is that most of these protocols are legacy, which emphasizes that their design did not include security considerations.

TABLE 3. Business impacts of cybersecurity threats filtered by risks.

Risks / Loss of	Attacks / Threats	Business impacts
Availability	Denial of service	Loss of production time Violation of commercial agreements with customers Quality degration of workparts Service theft
Integrity	Sabotage of the critical infrastructure, machines or components	Damage to working machines Quality degradation of products Violation of standards and regulations in the field of safety Violation of commercial agreements with customers on products
Confidentiality	Theft of industrial secrets, cyber-espionage	Reduction of company competitive advantage Damage to company image or reputation Violation of commercial agreements with industrial partners on data

Some common attacks against integrity are Man-In-the-Middle attacks, which consist in altering and relaying the communications between two entities, while the latter think they are directly connected.

c: CONFIDENTIALITY

Threats related to confidentiality consist in accessing or stealing sensitive data related to industrial processes, configurations, customers and administration. They can be labelled as cyber espionage. They are conducted through several scenarios, such as passive analysis of the network traffic, active code injection into operational applications to get security credentials or corruption of the control measurements.

d: AUTHENTICATION

This is concerned with the threats that take advantage of design flaws or software vulnerabilities to escalate privileges, and gain access to protected resources. Such attacks use social engineering techniques like phishing or chains of spam letters to collect strategic information. The misconfigurations leading to unsuitable access at both the physical and the logical level, can involve the same security issues.

B. BUSINESS IMPACTS

Cybersecurity threats are a serious subject, and they put the capabilities of the most advanced companies to the test. The year 2017 was a turning point because three high scale attacks occurred in the world [22]:

- NotPetya spread to 65 countries, and caused USD892 million in damages;
- Bad Rabbit which targeted critical infrastructures;
- WannaCry spread to 150 countries, and caused USD8 billion in damages.

The companies infected by these attacks stopped production for a long time, and could not fulfill their production operations efficiently. The impact of such threats is not just technical or financial. It can affect relationships with partners, and leads to judicial consequences. Table 3 reports the analysis found in [23] of the business impacts filtered by risks. All risks are covered by a range of threats, and it can be observed that the number of business impacts is greater than the number of threats. For every single threat, multiple business impacts occur, which suggests that no threat should be underestimated.

C. MAJOR SECURITY THREATS IN INDUSTRY 4.0

The major security threats faced by an industry 4.0 factory can be classified into the following categories [20]:

1) CYBER ESPIONAGE

Due to smart and connected business processes, industry 4.0 is vulnerable to cyber espionage. Well organized groups of cyber criminals have made industry 4.0 their favourite target to steal sensitive information and intellectual property. One of these groups is Black Vine group which targets mainly aerospace, energy and healthcare industries. The theft of corporate and product data is becoming very common, especially the software and functionalities that are easy to copy. In industry 4.0, the cooperation of multiple partners, such as suppliers in the network, makes the task easier for these criminals as their attacks can have many pathways and spread very fast.

2) DENIAL-OF-SERVICE

The Denial-of-Service (DOS) or Distributed Denial of Service (DDoS) is a cyber attack which aims to make the system unavailable. It can be achieved notably by:

- Launching waves of requests on a server to consume all its resources;
- Passing malformed input data to crash a process;
- Virus infiltration;
- Destroying or disabling the sensors in a system.

Most devices are interconnected in a factory, and by extension are interdependent. As a consequence, the unavailability of some devices can be very critical for a production environment, thus making these attacks very popular. Moreover, with cloud computing development, new ways to launch DDoS attacks appear, thus pushing companies to consider it with increased attention.

TABLE 4. Threats and risks by perimeter in a factory.

Risks / Loss of	Attacks / Threats	Business impacts
Availability	Denial of service	Loss of production time Violation of commercial agreements with customers Quality degration of workparts Service theft
Integrity	Sabotage of the critical infrastructure, machines or components	Damage to working machines Quality degradation of products Violation of standards and regulations in the field of safety Violation of commercial agreements with customers on products
Confidentiality	Theft of industrial secrets, cyber-espionage	Reduction of company competitive advantage Damage to company image or reputation Violation of commercial agreements with industrial partners on data

Contrary to cyber espionage where the loss is about virtual data, DDoS attacks have physical impacts with material damage such as the servers that might need to be replaced (overload), reconfigured or redesigned.

Another issue with these attacks is that they are unpredictable, and very difficult to control.

3) SUPPLY CHAIN AND EXTENDED SYSTEMS

To make the supply chain more efficient, the industry 4.0 paradigm features the connection across multiple organisational environments. However, the supply chain has inherent system vulnerabilities which can be exploited by attackers.

One vulnerability may be a supplier which is victim of a phishing attack or credentials theft, resulting in a massive data exposure for the factory.

4) SMART SECURITY AND SMART FACTORY

Most of the manufacturing companies are not fully aware of security risks that came with the industry 4.0 paradigm. Usually, they mainly handle the security issues when a serious incident occurs.

However, technical products alone are not enough to handle these risks. The human factor is an important point. Awareness of the employees regarding security is also important, from the skilled machine operators to secure software and planning engineers. This awareness can be achieved through multiple ways, such as:

- Awareness raising campaigns involving the complete manufacturing environment;
- Research groups in higher education institutions who study cybersecurity topics, and deliver guidelines to industrial professionals.

5) ADVANCED PERSISTENT THREATS

Advanced persistent threats (APT) belong to a specific class of cyberattacks. They are perpetrated by some groups with significant experience and resources. The concept is to take advantage of vulnerabilities to infiltrate the victim's network and stay unnoticed during a long period of time [14].

The first identified APT in the industry was Stuxnet in 2010. Stuxnet was designed as a platform to target PLC and SCADA in order to automate electromechanical processes and cause material destruction. It exploited zero-day vulnerabilities in Microsoft Windows operating system and Siemens software. Other examples are Duqu, DragonFly, BlackEnergy and ExPetr. The attack process followed by these APT is usually divided into five steps:

- Recognition of the network to find the vulnerabilities;
- Communication to start the first intrusion by sending exploits to the victim. It can be done directly with social engineering (phishing, etc.), or indirectly by compromising a third party such as the provider;
- Tracking of zero-day vulnerabilities to execute remote actions by using the backdoors of the previous steps;
- Propagation to other areas of the network to infiltrate new devices, in order to collect information or modify existing hardware behavior;
- Filtration of the obtained information to transfer them to the attacker domain.

The first step is possible due to metadata leakage coming from the servers, PLC and sensors. These issues are inherited in the cloud and IoT paradigms, and they must be addressed.

D. VULNERABILITIES, THREATS AND RISKS BY PERIMETERS

In this section, we analyze security flaws in the different predefined perimeters of the factory. Table 4 will be used as a support in the following sections.

1) MANUFACTURING-PRODUCTION

The critical equipment in the manufacturing area can be reduced to the ICS. From a proprietary and isolated architecture, ICS have become an open and standard platform highly interconnected with the corporate and public networks [15]. New features such as remote access to networks and devices has appeared, thus making possible a wide range of cyberattacks. Moreover, these systems are now available over the Internet.

From 1997 to 2015, the number of vulnerabilities rose from 2 to 189 according to the Kaspersky report in 2015 [15]. Most of the vulnerabilities in production are called zero-day because the developers just discover the existence of the flaw, while a patch to fix has not been released yet.

The usual reasons behind this are highlighted in [10]:

- In factories, the devices run for weeks or months without any security updates or antivirus deployment;
- Multiple pathways for intrusion (laptops carried in and out, USB sticks, etc.);
- No isolation between the different networks.

In this area, the most common threats intend to compromise availability and integrity, notably by physical destruction, DDos attacks, Malware and worms, zero-day attacks.

Physical destruction can enter the category of typical sabotage of industrial equipment. In the manufacturing area, DDoS attacks mainly focus on the routing with relay attacks, selective forwarding, grey hole, black hole or botnets which will affect availability.

Malware and worms will slow down operational performance to get sensitive information or to modify equipment behavior in order to compromise integrity. Behavior modifications can take many forms, such as the alteration of the communication protocols by exploiting their weaknesses regarding authentication and data integrity.

Passive traffic analysis can also be used to steal confidential information. The method used can be the injection of code in operational applications to corrupt the control measures, perform end user piracy, and then access the data.

Privilege escalation can be achieved by taking advantage of security flaws in the software. In 2015, IBM X-Force research reported that 45% of all attacks focused on unauthorized access.

The easy mobility of in-plant operators and their numerous interactions with mobile terminals (laptops, smartphones, tablets) increase the risks related to these threats.

Configurations and access controls of the applications and devices must be checked rigorously in this area.

2) LOGISTICS

In the Logistics area, there are numerous wireless devices which have some vulnerabilities, such as [24]:

- Wifi networks, especially when not encrypted;
- Business applications that still use HTTP protocol;
- Installing of malicious applications.

Network vulnerabilities (unencrypted wifi, HTTP, etc.) expose almost all information sent by the devices to hackers. For handheld terminals, all data scanned with the bar code scanner such as references, serial numbers, destinations of the products, as well as information about the IT infrastructure, such as the servers and the databases, are concerned.

Installation of malicious applications could be the source of malware attacks. As an example, HummingBad and HummingWale affect android devices, and deploy applications for collecting personal data that are sold along the way.

3) ACTIVE SUPERVISION

The Active Supervision area belongs to the corporate network and includes mostly desktop hardware. Some possible flaws in this area are [15], [24]:

- The absence of antivirus software or signatures that are not updated could infect all the ICS through the Internet, and make it unavailable;
- People not sufficiently attentive to security, who click on malicious links;
- Computer not locked when leaving the office;
- Access to unauthorized files/websites/data;
- Connection of external devices;
- Installation of unlicensed/hacked programs.

These previous vulnerabilities could be the source of several threats such as:

- Social engineering attacks (phishing);
- Attacks over the network;
- Virus, malware, worms, and ransomwares;
- Hardware and data theft, loss or break;
- Data transfer from and to unauthorized devices.

4) RESEARCH AND DEVELOPMENT

This area contains innovative equipment that can become the source of potential threats due to the lack of perspective on the technologies used. This area can also be the target of attacks due to confidential and valuable information that the attackers could find.

5) LIVING AREA

In the living area, the main equipment retrieved is VoIP phones. Even if VoIP saves on network costs for companies, it also brings new security threats and risks. Some of these risks are common, such as DoS attacks that overwhelm the VoIP server with Session Initial Protocol (SIP) call-signaling messages. Such attacks are dangerous because they do not necessitate a penetration of the whole network.

Viruses and malwares can also affect VoIP phones because VoIP configurations use softphones. With VoIP networks, mobile malware is also an issue because many users make VoIP calls with their smartphones. This means that, once the malware infiltrates the smartphone, it can access and steal valuable information.

Another threat is ''vishing'' which is the voice-based counterpart of malicious email phishing. Employees, suppliers and clients are tricked into sharing sensitive information.

Phreaking is when a hacker accesses the business VoIP network, and uses it in order to steal business data, change the network plan or make expensive calls, thus causing expensive service provider bills.

Eavesdropping is also a common cybersecurity threat which is very challenging to overcome. The hackers succeed in accessing VoIP calls and listen to them by capturing unencrypted VoIP traffic. In this way, they are able to perform identity theft, and also VoIP service theft.

The last threat is Spam Over Internet Technology (SPIT). For the hackers, it consists in capturing thousands of VoIP IP addresses, and then sending voicemail to a VoIP system.

6) EXTERNAL AREAS

External areas are divided into two categories which are physical and virtual.

a: PHYSICAL

The physical external area is made up of surveillance IP cameras, which belong to the Internet of Things. Threats for these types of devices are:

- Influence of the routing protocol operation mode with jamming and interference in order to disrupt the communications.
- Exhaustion of resources by using vulnerabilities in software that control the devices or with malicious code (malware).
- Manipulation of routing information to influence the traffic, as in a Sybil attack [14]. These attacks are gateways to others, such as black hole or DoS.
- Side-channel attacks to expose device information (battery, memory) or routing information and topology to identify vulnerable equipment in the infrastructure.
- Injection of dummy/fake nodes capable of executing code or injecting illegitimate traffic in order to control large areas of the network or perform eavesdropping.
- Poor access control causing unauthorized access to protected resources.

b: VIRTUAL

The second category is the virtual external area which regroups everything related to cloud computing. This latter is interesting due to the low cost investment, and the easy deployment it offers to companies. Many organisations use cloud computing as storage for their data, and also to host some processes. It can even be used in IoT to acquire sensor data, but also as a way for customers to manufacture a product through a shared network of suppliers throughout its life cycle. Behind these innovations appear these threats:

- DDoS attacks by using vulnerabilities inside scheduler component of some hypervisors to charge the service, and make it unavailable [14].
- Malware injection to replace a legitimate cloud instance service like a virtual machine, with a malicious one to get access to exchanged data.
- Side-channel attacks which stress machines to study electromagnetic emanations and access their resources.
- Shared memory attacks which analyze cache or main memory to get technical information about the infrastructure, running processes or to access the memory dump of virtual machines.
- Social engineering attacks which capture information from the clients of the different applications. The objective is to get sensitive data such as accounts, passwords in order to host malicious services in the cloud.

Most of these attacks are part of advanced persistent threats (APT), which can be performed mainly by attackers with experience and resources.

V. CYBERSECURITY SOLUTIONS FOR FACTORIES

This section will afford a detailed review of some existing solutions against cybersecurity threats. These solutions have been selected in order to present the main trends regarding the classical and innovative solutions that may apply in the different perimeters defined in this paper.

The following two notions are necessary for a better understanding of the presented solutions: countermeasures, and long term solutions from the literature.

A. DEFINITIONS

1) COUNTERMEASURES

Countermeasures can be seen as the short term way to defend against a threat or an attack. They represent a set of actions and techniques to eliminate a threat or prevent it, in order to limit the harm that it could cause. They can also help to report the threat so that corrective action can be performed [10].

2) SOLUTIONS

Solutions are the long term way to deal with threats. They are often defined with different names such as approach, methodology and architecture. They represent a complete set of actions protected against different types of cyberattacks. These solutions can be classified into three categories [15]: security evaluation tools, intrusion detection and prevention technologies, and also ICS risk management.

Security evaluation tools are able to provide safe experimentation with realistic test scenarios (attacks, infections, etc.) in order to spot security issues before production.

Intrusion detection and prevention technologies highlight the approaches to secure ICS by introducing new components or by upgrading the existing architectures. ICS risk management proposes guidelines, standards and metrics for ensuring security protection implemented against evolving threats.

B. CYBERSECURITY COUNTERMEASURES

According to [10], the following three-level approach can be used to guarantee the security of industrial control systems:

- Perimeter hardening by isolating plant network from the office network, using firewalls and DMZ;
- Multi-layer defense on the network to contain attacks;
- Isolate remote users in a separated zone/network.

These measures allow protection against unwanted accesses from and to the Internet, but are also used to separate services and areas between the systems in the factory. Encryption is the most popular of these measures and is available at multiple levels:

- Encryption of communications to avoid tampering and information disclosure;
- Encryption of stored data to avoid repudiation attack;
- Encryption of data streams to avoid all previous issues.

To be efficient, all countermeasures must be continuously updated,including encryption protocols, firewall signatures, security controls (patches), monitoring (logs analysis). Table 5 describes the most popular countermeasures summarised from [10], and how they can help in preventing cyberthreats.

TABLE 5. Countermeasures for cybersecurity in Industry 4.0.

Countermeasures	Protect / Prevent from
Encryption of communication	Data tampering Information disclosure
Encryption of stored data (digital signature)	Repudiation attacks
Encryption of data streams	Data tampering Repudiation attacks DDoS threats
Firewall / gateway and proxy	Unwanted network access (from/to)
Access control / multiple authorization	Unauthorized access (information, physical areas)
Software updates	Vulnerabilities (OS, business apps, firmware)
Secure communication (VPN, WI-FI and IP)	Eavesdropping Unauthorized connection Data analysis
Antivirus and malware	Malicious software

C. CYBERSECURITY PROPOSALS REVIEW

This section will highlight and present in detail some of the current cybersecurity solutions available in the literature (see table 6). For each solution, we report its purpose and design structure, and also the value that can be given to this solution.

1) CONTROLLED INDUSTRIAL ENVIRONMENT RESEARCH

a: PURPOSE

Modern companies require both logical and physical solutions for their information security. Despite the efficiency of logical controls, they are virtual and there is an interface which can get out of the system control and compromise it. This interface may be a human, and the breach appears when information is exchanged verbally. Moreover, the explosive growth of wireless networks in information system architectures has increased the possibility of information leaks even more [25]. For these reasons, [22] proposed to create a physical information security. This solution takes the form of "Protected Areas" (see Fig.5), which are spaces where sensitive and valuable data can be safely exchanged acoustically or visually.

b: DESIGN AND APPROACH

This solution has the following objectives:

- Prevent access to unauthorized people;
- Stop information spread at protected areas walls;
- Homogeneously protected and controlled environment.

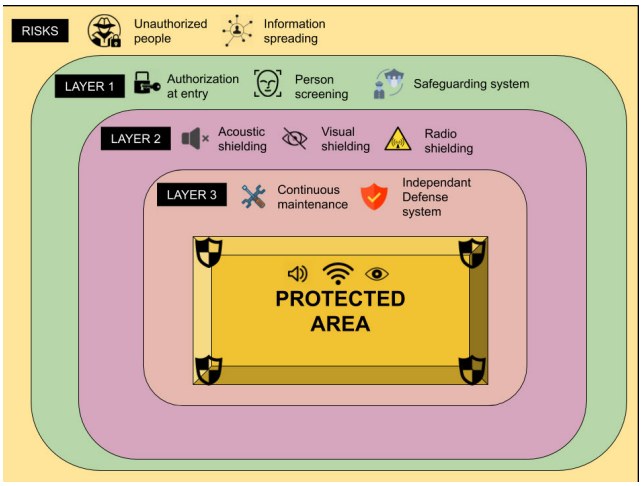

FIGURE 5. Protected area for controlled industrial environment research.

To achieve these goals, three layers of solutions are proposed. The first layer is made of conventional methods used for the defense of protected facilities: authentication at entry, people screening, definition of authorizations, and safeguarding systems.

With the first layer, we can be sure that only authorized people are in the area, but there is still a risk because information can still be "seen" from the outside.

The second layer helps to prevent the spread of information outside the protected zone through physical characteristics (visual, sound, radio) using acoustic shielding, visual shielding and radio shielding.

The last layer is dedicated to maintenance in the context of this security proposal, which proceeds through continuous maintenance and an independent defense system.

The idea behind the maintenance is to keep the homogeneity of the environment, search for foreign objects and monitor radio signals. A self-sustaining, safeguarding and monitoring system was also advised to complete the security of these protected areas.

c: FINDINGS AND VALUE

The author suggested that even if new technologies introduce new threats, the preparation and creation of these controlled areas among other actions could allow the maintenance of integrity, confidentiality and availability in the long term.

2) SOFTWARE DEFINED NETWORKING FIREWALL FOR MANUFACTURING EXECUTION SYSTEMS (MES)

a: PURPOSE

Manufacturing execution system (MES) is the intermediate system between ICS and corporate applications such as the enterprise resource planning (ERP). It improves the transparency of the manufacturing data. Sensor data can be used to calculate performance indicators in real time or to monitor the

TABLE 6. State of the art of cybersecurity solutions for Industry 4.0.

	Equipment concerned	Protect from what ?	Factory perimeter(s) concerned
Protected areas for controlled industrial environment	All	Unauthorized physical access, Information spreading (acoustic, visual, radio)	All
Software Defined Networking	Manufacturing Execution System (MES)	Network scanning / probing	MAN
Ontology Framework for IoT	IoT devices	External attacks (virus, data theft, security flaws)	MAN / LOG
Direct-To-Machine approach for CPS	Cyber-Physical systems (CPS)	Unauthorized instructions to manufacturing devices	MAN
Ensemble Intelligence Framework for advanced manufacturing	Industrial Control Systems (ICS)	Predictive detection of cyberattacks by using neural networks	MAN
Behavioral models, critical states with distance notion for ICS	Industrial Control Systems (ICS)	Predictive detection of cyberattacks by using distance notion and critical states (ex : sabotage)	MAN

status of the machine and quality of manufacturing processes. The enhancement of IT system interconnectivity exposes devices like PLC to cyberattacks, which could disturb production or infect other systems. Most common attacks in the case of MES are based on network scanning / probing where defence-in-depth is an effective countermeasure. Cybersecurity standards usually proposed network architectures divided into multiple segments with firewalls between them to minimize security risks. Considering the need to define configuration rules in a flexible and secured manner, the software defined networking (SDN) is likely a key technology in this regard [26], [27]. Another recent related proposal focusing on network performance is presented in [28]. SDN is a technology which can alternate the network, unlock critical intelligence and help deliver new services to run on-demand applications. It gives a clear overview of the network architecture to administrators and allows users to control the network architecture programmatically. That means it is be possible to modify the network access on demand, and minimize the exposure of ICS networks to attackers. In this context, [29] has proposed a protective network structure based on a SDN firewall specifically designed for industrial networks, without compromising network flexibility (Fig. 6).

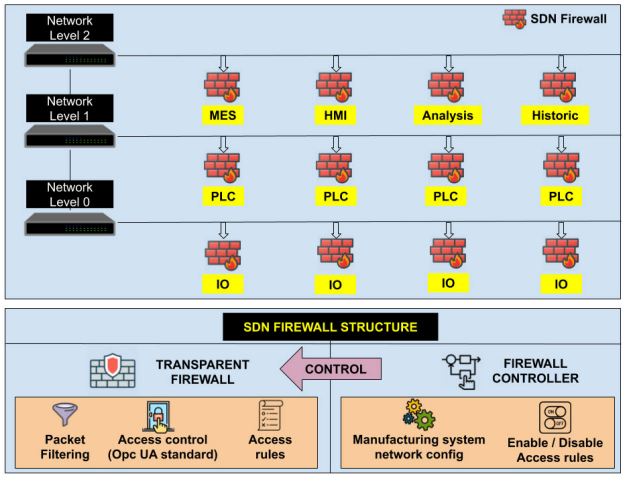

FIGURE 6. Software defined networking firewall for manufacturing systems.

b: DESIGN AND APPROACH

The proposed solution targets three objectives:

- Creation of segments without reconfiguring existing networks, while using a DMZ vertical integration.
- Development of unidirectional access mechanisms (access to server only when a client needs a connection).
- Reduction of loopholes in access rules due to frequent device insertion or replacement in some areas.

The SDN firewall has two main functions, which are:

- Packet filtering based on access rules application to a group of devices automatically.
- Bridge between network interfaces to avoid any change in the existing network configuration.

This packet filtering function means that only the applications that are in a white list can access industrial control devices. The white list is managed by network administrators, whose management task is greatly simplified, as this is the only thing to do in order to comply with security standards for ICS. With regard to the components, the firewall contains:

- The transparent firewall which enforces access rules and implements an access control system based on OPC UA standard.
- The firewall controller which keeps the configuration of the manufacturing system, and manages the rules.

The OPC UA standard (Open Platform Communication Unified Architecture) used in the access control of the

transparent firewall is a machine-to-machine communication protocol for industrial automation.

It is an evolution of the original OPC protocol which is better suited to meet emerging needs of industrial automation for Industry 4.0. Its most notable innovations are:

- Multi-platform implementation;
- Scalability (smart sensors, smart actuators, etc.);
- Multi-threaded or single threaded;
- Improved security (new standards);
- Configurable time-outs;
- Chunking of big datagrams.

The security in OPC UA consists of authentication, authorization, encryption and data integrity via signatures. Moreover, the communication stack uses firewall-friendly transmissions, which explains why this standard was used to design the SDN firewall.

c: FINDINGS AND VALUE

The author confirmed that the solution was tested in a virtual network of a complete environment (OPC client/server with exchange of machine data), and the firewall was able to prevent security scanners from acquiring application port and other OS level details of the OPC server.

The prototype implementation was able to complement security features in the OPC UA standard, and provided a holistic security solution for ICS networks.

3) CYBERSECURITY FRAMEWORK FOR IoT

a: PURPOSE

Internet of Things (IoT) is a term which associates multiple technologies related to sensor development and machine control. In the context of Industry 4.0, they are becoming popular due to interconnection between data from the industrial shop floors, and the possibility of providing run time feedback from the systems. Their usage leads to the new concept of Cyber-Physical Systems (CPS), which are associated with IoT implementation, and refer to the use of sensors to gather data, process them and use them in the cyber world. The main drawback which impedes their complete adoption is their weaknesses regarding cybersecurity, which is due to the heterogeneous connectivity and resulting threats (privacy violation, etc.), and may bring about major consequences to IoT technology users [30]. According to [31], these systems should be designed and operated under a unified view of safety and security characteristics. In the context of the smart factory, one of these threats could result from the weaknesses related to the use of cloud computing. Considering this situation, an ontology-based cybersecurity framework for IoT was proposed by [32].

b: DESIGN AND APPROACH

The proposed framework focuses on:

- Company-side monitoring.
- Security analysis and classification in a knowledge base.
- Security service design.
- Improvement of security mechanisms regarding business processes and technology assets.

Figure 7 is a representation of the framework architecture. It is divided into three layers: two layers dealing with cybersecurity at design and run time, and the integration layer used at both steps. The concept of the design layer is the following: it is supposed that a company needs to implement specific services at any time in addition to those already in use, which requires adaptation to meet device constraints.

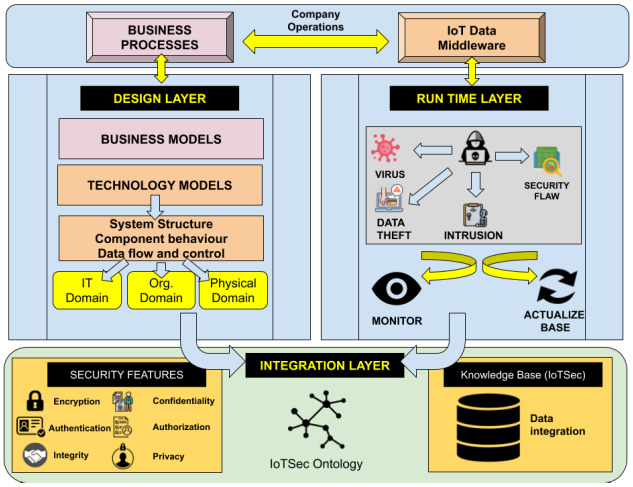

FIGURE 7. Ontology framework for IoT cybersecurity.

The MDSEA (Model-Driven Service Engineering Architecture) is a software development methodology which focuses on creating and exploiting conceptual models (in the case of the framework: business models, technology independent and specific models) related to a specific problem. By using this methodology, the design layer is able to generate code from high level of abstraction to accelerate the service design and adaptation, and also the deployment time. Then, company managers can collaborate with developers to participate in the creation of the new functionalities.

The run time layer has two objectives: monitoring and updating the knowledge base. Monitoring consists in detecting intrusions, data theft, viruses, and other attempts of security flaw exploitation. All these situations are analyzed to identify the suitable solutions from the pool of security services of IoTSec in order to recover the system and improve cybersecurity. The updating consists in adding detected threats and security analysis to the knowledge base, thus preventing those threats to appear again. The data integration layer provides information about threats and vulnerabilities using the IoTSec ontology, which is a continued work of [33].

c: FINDINGS AND VALUE

Finally, the authors consider that ontology in cybersecurity improves effectiveness in security operations, and helps analysts to extract relevant information to characterize the vulnerabilities. However, some open issues still exist before obtaining a multi-layered cybersecurity intelligence ontology

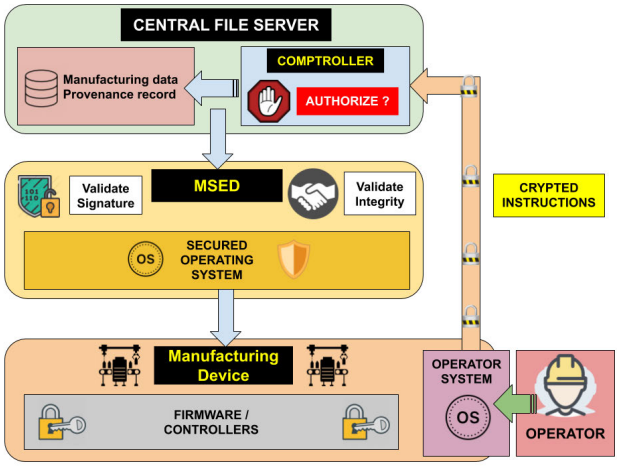

FIGURE 8. Direct-to-machine approach for cyberphysical system in manufacturing.

able to understand potential threats against the cybersecurity landscape, which is always changing.

4) DIRECT-TO-MACHINE APPROACH FOR CYBERSECURITY IN CYBER-PHYSICAL SYSTEMS

a: PURPOSE

Long value chains are one of the biggest security concerns in Industry 4.0. Information Technology (IT) paradigms do not reflect the particular circumstances encountered in the Operation Technology (OT).

Many types of data are accumulated during the production part, and are used for quality checks and predictive maintenance. However, only some of them are critical for protection. An OT solution should focus on: bill of materials, design information and control parameters [34].

In the manufacturing environment, the architecture currently in use is typically entirely separated from the production environments, with manufacturing devices air-gapped. There is no control over subcontractors in multi-step manufacturing when data leaves the server.

In the same way, the operators are unsupervised once data is received and many issues arise, such as data corruption. As it was established by [35], the threats exposed in additive manufacturing stretch across digital manufacturing devices of all shapes and sizes. Therefore, a new paradigm is proposed by [34]. It intends to limit and protect information flow in subcontracted floor devices to complement perimeter security.

b: DESIGN AND APPROACH

This new manufacturing information architecture is based on the holistic approach that data should be sent directly to the relevant manufacturing device. This approach is also called Direct-to-Machine communication (see Figure 8). The fundamental security problem behind this is about authentication and authorization:

- Is the request sent to the device authentic?
- Is the actor authorized to send this request?

To solve this issue, the proposed architecture is made up of two components. The first one is the Encryption with a Manufacturing Security Enforcement Device (MSED). It relies on asymmetric cryptography. The public key is used to verify that the actor or entity actually has the appropriate private key, thus authenticating it.

The second one is software called comptroller that runs on a manufacturing network and authorizes each action taken. It takes input data, provides a key and stores output data. The output data are added at the end of a virtual document which is the record of provenance for a produced part. Then, the transmitted data between the comptroller and the manufacturing device will be handled by a Manufacturing Enforcement Device (MSED), of which the complete overview can be found in [36]. The MSED sits in front of the manufacturing equipment and authenticates manufacturing instructions coming from the cloud by verifying both instruction data integrity, and comptroller identity and authorizations. To that end, the best method is to use encryption and unique data signatures ensuring that the data source is authentic. Another requirement for the MSED is to have a secure Operating System (OS). Common OS for embedded systems are Microsoft WindowsTM or LinuxTM. They provide a large range of tools, but are vulnerable to zero-day attacks which can be devastatingly effective. The authors [34] mentioned smaller OS such as SeL4, which was formally verified to be secure.

c: FINDINGS AND VALUE

A prototype MSED device using the SeL4 micro-kernel was completed with "True Secure SCADA, LLC", and was confirmed compatible for general industrial control as well as manufacturing.

The direct-to-machine communication has solid arguments to overcome cyber-physical security challenges, notably:

- its characteristics (authorization, monitored operator control, device support, distributed responsibility, location independent).
- its contrast with existing solutions (integrated security, layered encryption, always up-to-date, integrity protection, minimum sharing).
- its role in building responsive manufacturing environment (detailed tracking with comptroller, collaboration, distributed manufacturing, automation).

One of the challenges regarding the adoption of this approach is the will to handle cyber-physical security rises, or that IT departments recognize manufacturing equipment as another digital component in the protects. In Industry 4.0, these devices are no longer separate from the data flow, and the direct-to-machine approach acknowledges that fact.

5) ENSEMBLE INTELLIGENCE IN ADVANCED MANUFACTURING

a: PURPOSE

Traditional cybersecurity architectures focus on mechanisms that provide confidentiality, authenticity, integrity, access

control and non repudiation in order to prevent network intrusions and attacks. However, the current security landscape is characterized by attacks which constantly evolve, and are voluminous, fast, persistent and highly sophisticated.

For critical systems belonging to Industry 4.0, the need for autonomic detection and response to cyberattacks is necessary in order to get a robust cybersecurity with in-depth-defense. A cyberattack detection algorithm was proposed by [37] to defend Industry 4.0 systems, as well as other Internet-driven systems. It is based on ensemble intelligence with neural networks to operate a classification output providing feedback to active response mechanisms. The underlying objective is to show how computational intelligence approaches can be used in the Industry 4.0 cybersecurity.

b: DESIGN AND APPROACH

Usually, cyberattack detection systems require algorithms that collect and analyze data generated by various events occurring within a cyber environment. One of their main issues is the lack of accuracy, and inaccurate results can impact the system performance negatively and lead to security issues (false alarms, unnoticed intrusions, etc.).

Computational intelligence Systems (CIS) are adaptive systems with decision making capabilities, and they are specifically designed to handle large volumes of noisy data in their decision process. Therefore, they seem to be a logical choice when designing new algorithms for detection systems. These systems use technologies such as machine learning and deep learning which are able to accurately discover essential differences between normal data and abnormal data [38], [39].

The proposed algorithm is called Neural Network Oracle (NNO) classification algorithm, and it is made up of three components: neural networks, genetic algorithm and Neural Network Oracle.

Figure 9 is a representation of the ensemble intelligence framework which uses the NNO classification algorithm in the context of predictive detection of cyberattacks for advanced manufacturing.

Neural networks also called Artificial Neural Networks (ANN) are inspired by biological processes, and are used to solve artificial intelligence problems. One of their most interesting features is self-learning based on training with data. In the NNO, a collection of neural networks will train with a first set of audit data. Then, the output of this first classification will be sent to the NNO.

The genetic algorithm (GA) draws its inspiration from the biological evolution process, and the ability to adapt over time within changing environments. In the NNO algorithm, the GA is responsible for finding the most optimal parameters in order to reduce the error rate, and increase the accuracy. To obtain these optimal parameters, a fitness function evaluated with neural network responses is used.

The neural network oracle is trained with a secondary set of data made up of outputs from the previous neural networks,

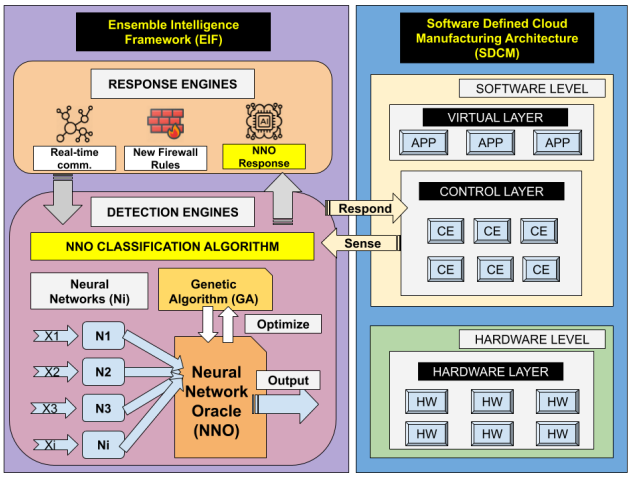

FIGURE 9. Cyberattack predictive detection with ensemble intelligence in advanced manufacturing.

and the original set of data. To minimize errors, it uses the optimal parameters provided by the genetic algorithm.

c: FINDINGS AND VALUE

The author integrated the ensemble intelligence framework based on NNO classification into a Sofware-Defined Cloud Manufacturing Architecture (SDCM) [37]. The SDCM is divided into 3 layers: virtual, control and distributed hardware.

As the control layer is the one with the deepest insight into activities and communications, it will be used as data tap points. The control layer will feed the Ensemble Intelligence Framework (EIF) with streaming data, and the EIF will be responsible for analyzing sensed data and responding to the anomalies detected.

In terms of performance, the NNO was trained and tested with the CUP99 intrusion detection dataset, and it showed good classification performance. It was concluded that it could be coupled with active response mechanisms in the context of Industry 4.0 to stop cyberattacks.

6) BEHAVIORAL MODELS AND CRITICAL STATE DISTANCE NOTION TO PROTECT INDUSTRIAL CONTROL SYSTEMS

a: PURPOSE

Industrial control systems (ICS) have been increasingly targeted by hackers since the beginning of the 21st century due to potentially significant damage that they could inflict on the system and its environment in case of success. The ICS network can be divided into three levels [40], [41]:

- Level 0: Operative part with sensors/actuators;
- Level 1: Control part with PLC/HMI;
- Level 2: Supervision with control room/SCADA;

IT solutions such as firewall/DMZ are usually used in the level 2 and higher to protect from DDoS attacks or Man in the Middle attacks (MITM). The solutions in this layer work because it is very similar to traditional IT infrastructure.

However, these solutions do not work on real time layers 0 and 1, which have their own inherent attacks (random attacks,

false data injection). Four types of attacks are considered, namely direct, sequential, temporal and Over-soliciting.

An innovative methodology was proposed by [13], and is based on the concept of ''automation knowledge''. This is a deepening of [40] from the same author. The solution will be dedicated to protecting low level elements (level 0-1) like PLCs, sensors of the Computer-Integrated Manufacturing (CIM) architecture by taking into account safety and security aspects. The final objective is to be able to detect malicious orders sent by the PLC.

This approach can be considered as a last shield to protect the system from cyberattacks by supposing that the hackers have already crossed previous levels of defense.

b: DESIGN AND APPROACH: MODELS AND FILTERS

The first step is based on behavioral models [42], which represent the normal way of functioning of the system. It is divided into four parts:

- Risks assessment to determine critical areas to protect (Prerequisite).
- Parameter identification (Offline).
- Control filter model generation (Offline).
- Operation mode where detection mechanisms are performed (Online).

The risk assessment is a prerequisite. The methodology assumes that a risk analysis was carried out on the system. This analysis must highlight the events feared for the system and induce which part of the ICS must be protected as a priority (list of I/O to model). These I/O are the PLC inputs/outputs.

Parameter identification consists in creating the states based on the I/O list from the risk assessment. This will help to define both the perimeter and the states used in behavioral models. Mathematically, these states are defined with combinational constraints based on sensor and actuator values. The following types of states are considered in an ICS:

- Optimal states (Respect control law, physical system constraints).
- Dangerous (Respect only physical system constraints).
- Prohibited (Degrade physical system).
- Reachable (All possible states).
- Unreachable (Impossible states).

Then, temporal constraints must be determined to identify temporal attacks. These temporal specifications add another dimension to the characterization of the system behavior, and add another level of protection for the ICS. Usage of combinational and temporal constraints is needed to ensure efficiency of the detection algorithms.

The generation of the control filter model aims at modeling the industrial system with the process and control model. The operation step corresponds to the availability of both control and report filters in the ICS. These filters must be located just after the sensors to guarantee the integrity of the orders, and to detect any malicious behavior (see figure 10).

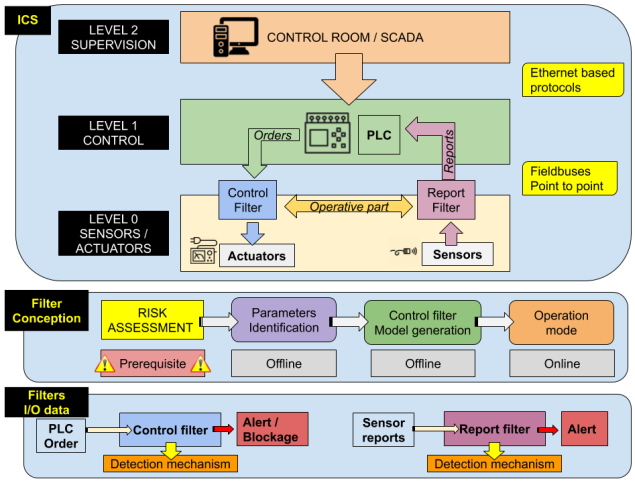

FIGURE 10. Filters overview (implementation, conception, role) in the behavior model approach for ICS protection.

The next question is to determine the protection level desired with these filters. Three layers of security are considered:

- Security of goods and people: guarantee a set of states where the system can evolve without danger.
- Quality: guarantees correct execution of the control law, and monitors the system.
- Equipment protection: monitors the solicitation of the actuators with orders that are too strong or frequent (to prevent fatigue, breakdown, and reduce maintenance on equipment).

c: DESIGN AND APPROACH: DETECTION BASED ON DISTANCE AND TRAJECTORY

The filters described in the previous paragraph allow the implementation of rules, but they can stop attacks only one step before reaching a critical state. A detection mechanism of deviations from normal behaviour is needed to complete the methodology. This mechanism is based on three notions, which are distance, shortest path to critical state and trajectory. Figure 11 is a simplified representation of the proposed detection mechanisms.

The notion of ''distance'' is related to the ICS states, and was introduced in [43]. It represents the gap between the current state and a set of critical states, which are all states that the system must not reach. This concept is very interesting because it gives indications to operators about the proximity with the critical area. The ''shortest path to critical state'' is the smallest number of orders which have to be applied before reaching a critical state. The general purpose is to compute, for every reachable state, the nearest distance with a critical state. These computations are done offline and integrated into the filters to perform the detection algorithm, while taking into account real time constraints. The last notion is ''trajectory'' which is complementary to the distance concept. Distance gives only punctual information for the system, but

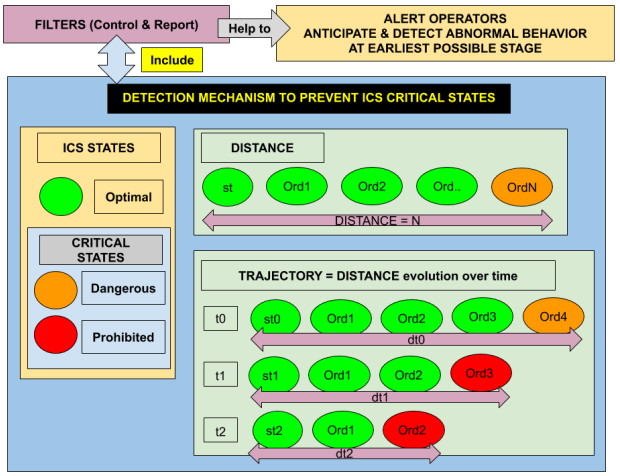

FIGURE 11. Detection mechanism based on distance and trajectory for filters to protect ICS.

trajectory is defined as ''the evolution of distance according to state sequence or time''.

The following detection mechanisms can be implemented with the distance/trajectory approach:

- Context detection;
- Anomaly detection (combinational and temporal);
- Equipment degradation.

The main advantage of the proposed mechanisms is to prompt operators, anticipate the deviations and detect abnormal behaviors at their earliest stage.

d: FINDINGS AND VALUE

The author confirmed that the approach showed good results for detection of cyberattacks that affect physical systems. The improvement was the blockage of the orders before leading the system into a critical state, and the detection of sequential attacks using combinational and temporal constraints. However, some improvements were suggested, such as:

- The use of a security/safety approach to improve efficiency and the number of attacks taken into account.
- Consideration of system evolution between two stable states.

D. HONEYPOTS AND OTHER INNOVATIVE SOLUTIONS

1) OVERVIEW

Several original innovative solutions are available in the literature, such as the immune system for cybersecurity in Industry 4.0 [44], to mention few. However, in this paper we will focus on two popular approaches: honeypots and digital twins. Honeypot systems are passive monitoring systems with early warning capabilities for production environments and critical infrastructure. Their core functionality is to give alerts if the infrastructure has been breached by hackers or malware-related activities. Technically, a honeypot consists of data that seem to be a legitimate part of the system with valuable resources for attackers. However, in fact, the honeypot is isolated and monitored to block or analyze attackers. Concretely, the honeypot concept is about baiting attackers. The main benefits from this solution are:

- Awareness of the fact that someone or something is trying to exploit your business critical systems.
- The attacker is wasting precious time attacking a fake system, instead of the real infrastructure.
- The security team has more time to stop the attack.
- Your company will not waste time on false positive alerts as there is no reason for any communication from or to the honeypot system.

2) HONEYPOT BASED SOLUTIONS

Existing honeypot-based solutions are usually distributed systems able to collect and analyse the information related to threats or attacks [14]. The purpose of this analysis is to determine the type of attack, the existence of infected devices, as well as the activities carried out on the system.

a: ThreatMatrix BY ATTICA NETWORKS

ThreatMatrix is the major existing honeypot-based detection platform able to detect real-time intrusions in ICS/SCADA systems, and in IoT environments [14]. Its flagship, BOTsink, is able to detect APT (Advanced Persistent Threats) without being detected by attackers. Some other features are also included such as software images to simulate SCADA devices and their protocols, and make them indistinguishable from real ones.

b: ICS HONEYPOT BY INDUSTRIAL DEFENICA

In 2018, a global study conducted by the Ponemon Institute on behalf of IBM found out that the average amount of time required to identify a data breach is 197 days. Moreover, the most famous attacks in industrial environments involved hackers in the network for at least three months. Based on these results, Industrial Defenica proposed a high interaction ICS/SCADA industrial honeypot.

This solution uses advance deception technology able to present fake units based on templates (PLC, Ethernet-to-serial device) on the network. More than 3500 various devices can be faked (protocols, services, open ports, etc.), and these faked devices can communicate with real ICS equipment. Many steps are necessary for attackers to determine if it is a real device, and these steps would alert the security team that someone is intruding into the infrastructure.

To provide the best possible threat data, a global ICS Industrial Honeypot network has been created to get feedback from deployed solutions, as well as to improve data, equipment support, better equipment profiles in order to maintain them as believable simulators.

3) DIGITAL TWINS FOR CYBER-PHYSICAL SYSTEMS

Digital twins was recognized as a top strategic technology trend in 2019 by Gartner [45]. Here, we focus on some use cases that show how they can strengthen the security of cyber-physical systems.

a: DEFINITION

The standard definition of digital twins is that they are virtual replicas of physical objects which make it possible to monitor, visualize and predict the states of cyber-physical systems [45]. In the context of information security, [45] proposed a uniformed definition based on the literature: a digital twin is ''a virtual replica of a system that accompanies its physical counterpart during phases of its life cycle, consumes real-time and historical data if required and has sufficient fidelity to allow the implementation of the desired security measure''. Another term is also mentioned regarding digital twins: the digital thread. In [45], digital thread is defined as ''the unbroken data link through the life cycle of a system that can be utilized to generate and provide updates to a digital twin''.

b: USE CASES IN MANUFACTURING DOMAIN

Multiple use cases were identified for digital twins role in securing manufacturing systems:

- Secure design of CPS;
- Intrusion detection;
- Detection of misconfiguration (hardware and software);
- Security testing;
- Privacy;
- System testing and training;
- Secure decommissioning;
- Security and legal compliance;

To design more secure CPS, the idea is to use digital twins in combination with a virtual environment in order to analyze how the system behaves under attacks. Thereby, engineers could estimate potential damage, thus facilitating the design process of security and safety mechanisms to produce more robust and fault-tolerant CPS architectures. Digital twins could also help to reveal weak spots in the architecture or unnecessary functionalities in the devices, which could expose them to an intrusion.

Digital twins can also help to implement intrusion detection systems (IDS). Indeed, [45] presented a passive state replication approach which aimed to replicate a state from a physical device to a digital twin. This allows the digital twin to mirror the behavior of the real CPS during operation. Then, it is required to implement a behavior-specification-based IDS where the CPS normal behavior is correctly defined to detect any modifications. This technique yields a low false-negative rate and can detect some attacks that were unknown at the time the legitimate behavior was defined. Finally, intrusions can be simply detected by comparing inputs and outputs of physical devices and their associated digital twins.

As digital twins are the result of a hardware and software emulation of devices, they mimic similar functionalities. The detection of misconfiguration in hardware and software consists in observing different behaviors between the digital twins and their physical counterpart. If a difference is observed, it could be indicative of malicious actions. Contrary to traditional configuration data analysis where only the software is checked, this use case also applies to hardware.

Security tests in OT environments are critical because they are conducted on live systems, and can cause severe damage or business interruptions. Normally, testbeds are used to avoid interference, but their maintenance is costly in time and effort. Digital twins make it possible to perform security tests virtually instead of conducting them on the real systems. Of course, fidelity of the digital twin is a critical point, and this use case could also apply to the engineering phase to fix vulnerabilities early in CPS. In operational phases, the use of a digital twin as a honeypot system could also make it possible to test the security of the CPS against real attackers, and help to reinforce the real CPS security.

The concept of digital twins can also help to protect privacy, for example in assisting the controllers or processors to meet General Data Protection Regulation (GDPR) requirements. For example, an insurer offering an insurance product based on the data obtained from the digital twins of smart cars. As the digital twins use some methods to classify data which can be anonymized prior to data transfer to the owner, then privacy rights can be preserved.

As digital twins are virtual and run in an isolated environment, they can be used as a testing and training platform. This platform could serve for testing new defense or to train on how to respond to cyberattacks. The main idea is to launch attacks against the digital twins from the virtual environment for testing and training purposes.

When the end-of-life of ICS and CPS is reached, the components must be disposed of in a secure manner. Multiple aspects must be considered, such as confidentiality requirements on data, as well as the costs associated with the sanitization. Digital twins could facilitate the secure disposal of physical devices. However, they may be affected by unauthorized access. Therefore, it is important that the digital thread be cut off and archived properly.

Regulatory requirements for operators of CPS seem to be increasing, that is why digital twins could help by providing an accurate reflexion of CPS through their entire life cycle to allow continuous monitoring and documentation of security aspects.

VI. CYBERSECURITY GUIDELINES FOR FACTORIES

This section will promote what we consider as guidelines for cybersecurity in Industry 4.0. To achieve that goal, the approach will be structured the following way:

- Guidelines mentioned in the literature.
- Standards and methodology from official organisations.
- Policies required to build a strong cybersecurity.
- Good practices (technical and organisational) summarized from multiple institutions.

The cybersecurity institutions considered in this section are ENISA (European Network and Information Security Agency), ANSSI (French National Cybersecurity Agency) and NIST (National Institute of Standards and Technology).

A. STATE OF THE ART

A general view of cybersecurity guidelines found in the literature was proposed by [10], and presented in four axes:

- Provide support for connected products;
- Define a security approach;
- Fix set of actions guaranteeing information security;
- Define/respect a specific policy when implementing new industrial security services.

1) SUPPORT FOR CONNECTED PRODUCTS

In manufacturing industry, support for connected products must be provided by the company in some specific fields:

- Cybersecurity consulting to get advice and guidance regarding strategy at the top level;
- Risk management to prevent cyberattacks;
- Threat monitoring to monitor and provide the tools able to detect cyber threats;
- Cyber incident response to prevent future attacks, and limit the damage;
- Training to limit likelihood of the attacks taking place;
- Cybersecurity packages related to products being sold (for example, a subscription could include anti-malware software as a service to offer monitoring, detection and training).

2) SECURITY APPROACH LEVELS

The definition of a security approach should pay attention to multiple levels, notably network, transport and application. The network level should provide a secure and trustworthy connection. The transport level will guarantee that transmitted information cannot be read, and will authenticate source and destination sides. Finally, the application level is supposed to ensure security on the information transmitted even if there is no encryption at the transport level.

3) SET OF ACTIONS FOR INFORMATION SECURITY

To guarantee information security, multiple actions should be performed:

- Ranging information sources;
- Classifying objects to protect;
- Description of threats arising in case of unauthorized access or change of information;
- Description of how to prevent unauthorized access;
- Description of how to fix information change and stop current unauthorized access.

4) POLICY FOR INDUSTRIAL SERVICES IMPLEMENTATION

When implementing new industrial security services, it is necessary to follow four steps:

- Design the service based on the knowledge of the automation system and its operational environment.
- Define the service operations addressing customer needs.
- Implement a DevOps approach able to integrate operational experience in the development process.
- Introduction of control loops into technical and economic systems of industrial companies, in order to bring the system back to a stable state after disturbance.

B. STANDARDS AND METHODOLOGIES

1) ISO/IEC STANDARDS

Most official institutions propose their cybersecurity recommendations by using standards as references. In the cybersecurity context, the most famous come from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Regarding cybersecurity in smart manufacturing and Industry 4.0, two standards can be outlined: ISO/IEC 27002 and ISO/IEC 27017.

a: ISO/IEC 27002

ISO/IEC 27002 contains the good practices and recommendations about information security controls by those responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS). The following subjects are detailed:

- Policies (IS security, HR, security organisation);
- Access control;
- Asset management;
- Cryptography;
- Security (Physical, operation, communication);
- Supplier relationships;
- Compliance.

These standards were used by ANSSI to establish its good practices checklists, which will be detailed later in this section. One of the downsides of ISO/IEC 27002 is the lack of a cloud approach with regard to security controls. That is why the ISO/IEC 27017 standard was created.

b: ISO/IEC 27017

ISO/IEC 27017 was developed for cloud service providers and users in order to make cloud-based environments safer. It consists of guidelines about implementation of security controls by cloud service customers, and by cloud service providers which support the implementation. It is complementary to ISO/IEC 27002 and addresses the following:

- Responsibilities between providers and customers;
- Removal or return assets at the end of contract;
- Protection and separation of customers virtual environments;
- Virtual Machines (VM) configuration;
- Administrative operations and procedures in cloud environments;
- Monitoring activity by cloud customers;
- Virtual and cloud network environment alignment.

Famous cloud platforms already follow these standards such as Microsoft Azure, Google Cloud Platform, and Amazon Web Services. Considering that these platforms are external and depend on different legal entities (countries for example), it is important that their customers be informed about the cybersecurity standards they are following.

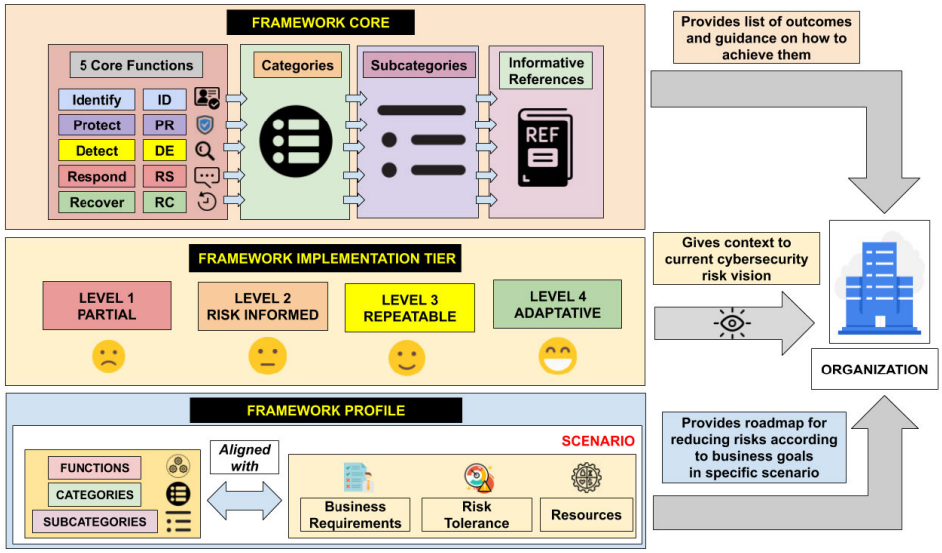

FIGURE 12. NIST framework structure overview.

2) NIST FRAMEWORK

In order to address and manage the cybersecurity risks related to industrial control systems, the National Institute of Standards and Technology (NIST) located in the United States of America has proposed a framework [46]. This latter is multi-platform and applicable to IT, ICS, CPS, and also to IoT. In addition to helping organisations to manage and reduce the risks, this framework will give them taxonomy and mechanisms to:

- Describe their cybersecurity posture;
- Describe their target state;
- Identify and prioritize opportunities;
- Assess progress towards the target state;
- Communicate among internal and external stakeholders about cybersecurity risks.

With regard to the structure, it is divided into three blocks, which are the framework core, the implementation tier, and framework profiles. Figure 12 gives an overview of the framework structure.

a: FRAMEWORK CORE

The framework core presents industry standards, guidelines and practices to allow the communication of cybersecurity activities and outcomes from the executive level to the implementation level. The core is made up of four parts, which are: core functions, categories, subcategories, and informative references.

Core functions provide a strategic view of the life cycle of the cybersecurity risk management by an organisation:

- Identify (ID);
- Protect (PR);
- Detect (DE);
- Respond (RS);
- Recover (RC).

Identify function is about determining the business context (systems, people, assets, data, capabilities), the resources with critical functions and their related risks in order to focus and prioritize the efforts.

Protect function consists in developing and implementing safeguards to ensure availability of critical services, as well as to limit impacts of potential cybersecurity events.

Detect function will implement the activities necessary to identify the occurrence of a cybersecurity event.

Respond function will implement the activities to take the actions regarding a detected cybersecurity event. It also supports the ability to contain the impact of a potential cybersecurity event.

Recover function will implement the activities aiming to maintain the plans for resilience, and to restore any service impaired by a cybersecurity incident. The purpose is to reduce the impact of the incident.

For each function, the core identifies discrete outcomes which are categories and subcategories.

Categories are groups of cybersecurity outcomes tied to programmatic needs and particular activities like asset management, detection processes or access controls.

Subcategories are divisions of categories and help to support achievement of outcomes in each category. Some examples are ''External information systems are catalogued'' or ''Notification from detection systems is investigated''.

Information references are standards, guidelines or practices that illustrate the method to achieve the outcomes associated with each subcategory.

b: FRAMEWORK IMPLEMENTATION TIERS

The implementation tiers give information about how an organisation views a cybersecurity risk, and which processes are deployed to manage this risk. Tiers describe an increasing

TABLE 7. NIST framework implementation tier levels.

N°	Level name	Risk management process	Integrated risk management program	External participation
1	Partial	No formalization of risk management practices and management in reactive manner (when attack occurs)	Limited awareness of risk at organizational level, risk management implemented on irregular basis	No understanding of its role in ecosystem, no communication with other entities and no information share. Unaware of cyber supply chain risks (products/services used or provided)
2	Risk Informed	Risk management practices approved, but not established as organizational policy	Awareness of risk at organizational level, but organizational approach not established. Information shared internally on informal basis	Understanding of its role with dependents or dependencies but not both. Receive information from other entities but no share of information. Aware of cyber supply chain risks but doesn't act formally upon these risks
3	Repeatable	Practices formally approved, regularly updated and organizational policy established	Organizational approach for cybersecurity risk, awareness of employees of their responsabilities, regular communication about risks	Understanding of its role with dependents and dependencies and contribution to understanding of risks with the wider community. Collaborates, receives and shares with entities. Act formally upon these risks (written agreements)
4	Adaptative	Practices adapted based on previous/current activities and predictive indicators. Continuous improvement, adapts to changing threat/landscape and responds in a timely and effective manner	Organizational approach to manage risks, roles between executive hierarchy levels are well understood. Organizational budget based on risk environment/tolerance, implementation of vision. Cybersecurity is becoming part of the organization culture.	Understanding of its role with dependents and dependencies and receives, generates, reviews and prioritizes information related to continuous analysis of risks and landscape evolution. Uses real time information to act upon cyber supply chain risks. Proactive communication (formal agreements and informal mechanisms) to maintain strong supply chain relationships

rigor and sophistication in cybersecurity management practices. They help to determine multiple things like:

- Knowledge of business needs by risk management;
- Risk management level of integration into organisation practices;
- Integration of privacy and civil liberty considerations into risk management and risk responses.

Table 7 summarizes the four existing Tier levels, and how they evaluate the cybersecurity vision of an organisation based on the risk management process, the integration of a risk management program and its external participation: partial, risk informed, repeatable, and adaptive.

The lowest level (level 1 ''Partial'') is considered to be an organisation which does not formalize risk management practices, has no awareness of risks at organisational level, and which does not understand its role in the ecosystem and in the supply chain risks (products and services used or provided).

Through these levels, organisations improve their cybersecurity management by formalizing practices and by becoming aware of risks at organisational level (level 2 ''Risk Informed'').

Then, they also establish organisational policy and start to collaborate, receive and share information with external entities (buyers, suppliers) at level 3 (''Repeatable''). Finally, at level 4 (''Adaptive''), they switch from a reactive approach to an active one by using the practices based on their experience and predictive indicators.

They adapt to changing landscape by using continuous analysis, and cybersecurity becomes part of the organisation culture. Their communication becomes proactive to maintain strong supply chain relationships. The tier selection process considers multiple aspects of an organisation:

- Risk management practices;
- Threat environment;
- Legal and regulatory requirements;
- Business objectives;
- Organisational constraints.

In Industry 4.0, the lowest acceptable level would be level 3 (''Repeatable''), but level 4 (''Adaptable'') is the optimal objective, while considering that awareness and organisational policy are mandatory for cybersecurity risks (level 3). However, at the same time, continuous improvement, analysis

and adaptation from level 4 are critical to deal with Industry 4.0 challenges.

c: FRAMEWORK PROFILES

The framework profile represents outcomes based on business needs that an organisation has selected from categories and subcategories. It can be considered as the alignment of standards, guidelines and practices in a particular implementation scenario. These profiles have multiple advantages:

- Identify cybersecurity improvements (compare current profile with a target profile).
- Flexibility, as new categories can be added and prioritized to address organisation risks.
- Conduct of self-assessments.
- Communication within or between organisations.

d: HOW TO USE THE FRAMEWORK

In order to use this framework, it is important to have a coordination among three levels inside the organisation: executive level, business process, and implementation level.

The executive level sends mission priorities, available resources, risk tolerance to business level. The business level uses previous information as inputs in the risk management process and communicates with implementation level to establish business needs and create a profile. The implementation level communicates the integration progress of the profile to the business level to perform an impact assessment. Then, this impact assessment is reported by the business level to the executive level for awareness of the risk management process. Once the coordination is well established, the framework can be used for identifying, assessing and managing cybersecurity risk. It was designed to complement existing operations, and not to replace them. Multiple usages exist for this framework and are described in its documentation:

- Review of Cybersecurity practices;
- Establishing or improving a cybersecurity program;
- Communication of requirements with stakeholders;
- Buying decisions;
- Identifying opportunities for new or revised informative references;
- Methodology to protect privacy and civil liberties.

C. POLICIES

To ensure a good level of cybersecurity, the first group of security measures consists in establishing policies and procedures. ENISA proposed a classification of the different policies required in companies regarding good practices for IoT in smart manufacturing [47].

1) SECURITY BY DESIGN

Security by design measures should be applied from the earliest stage of a product development. They are divided into the following points:

- Treat cybersecurity as a cycle with an approach from the perspective of devices and infrastructure;
- Address cybersecurity through embedded features, and not only at the network level;
- Equip every connected device, even the most basic, with identification and authentication features.
- Perform risk and threat analysis with cybersecurity experts from early stages of the design process of a device;
- Address security of all the information and control systems in every design document.

2) PRIVACY BY DESIGN

Privacy by design measures are related to protection and privacy of personal data. Like security by design, they have to be applied from the earliest stage of product development. They are divided into the following points:

- Address privacy issues regarding local and international regulations, such as the General Data Protection Regulation (GDPR);
- Define the scope of data processed by devices, and avoid collecting of sensitive data;
- Establish physical location of data storage;
- Conduct a Privacy Impact Analysis (PIA) about data processed by devices;
- Separate data which can be used to identify individuals, and secure them.

3) ASSET MANAGEMENT

Asset management measures are related to asset discovery, administration, monitoring and maintenance. They are divided into the following points:

- Usage of tools which are dynamically able to discover, identify and enumerate assets;
- Presence of an up-to-date and consistent asset inventory;
- Usage of active monitoring devices or passive ones (if legacy systems);
- Centralized asset inventory inside manufacturing plant;
- Dedicated management network for administration of assets;
- Introduction of new device only after communicating about changes in the management process;
- Avoid usage of removable devices.

4) RISK AND THREAT MANAGEMENT

Risk and threat management measures are related to the recommended approach to deal with risks and threats in Industry 4.0 environment, through the following points:

- Development of an approach considering new parameters, threats and attack scenarios dedicated to smart manufacturing;
- Determine risk management areas and assess specific threats and protection measures for them;
- Establish a risk and threat management process according to individual needs and security requirements;
- Perform risk analysis integrated with other processes regularly (at least annually) to monitor threats, and determine their impact on systems;

- Incorporation of threat intelligence within threat management by sharing information with trusted partners, such as ISAC and CERT.

D. ORGANISATIONAL GOOD PRACTICES

Organisation principles and governance are indispensable factors in terms of company security. They show how companies should operate, organisational rules and responsibilities which should be established, and the approach to use towards employees and third party contractors to handle cybersecurity incidents and manage vulnerabilities [47]–[49].

1) ROLES AND SECURITY ARCHITECTURE

All ICS should be covered by a chain of responsability where roles are clearly established, and security is based on an architectural approach. It is divided into the following points:

- Clear communication about roles for systems and security processes;
- Security architecture based on business requirements and aligned with risks;
- All relevant aspects are covered by security architecture (organisational and physical);
- Integration of compliance enforcement controls, and ensuring that the products meet defined requirements.

2) RISK ANALYSIS/VULNERABILITY ASSESSMENT

As mentioned in [10], the National Institute of Standards and Technology (NIST) recommended companies undertake a vulnerability assessment which is a process to identify and assess potential vulnerabilities of systems. To complete this definition, we can add that the vulnerability assessment is a systematic examination of an IT system to determine the adequacy of security measures, provide data to predict the effectiveness of these measures and confirm their adequacy after implementation. This assessment should be carried out by a certified service provider.

In addition to this vulnerability assessment, there should be regular risk analysis updates when new vulnerabilities are found. The NIST framework, already detailed in this paper, is an excellent tool to do this analysis. Risk analysis can also help to classify and prioritize security objectives. Figure 13 shows the flowchart to classify the risks during risk analysis. It can be used as a complementary tool with the NIST framework.

3) INVENTORY

Inventory is another key component of a good cybersecurity policy as it provides a complete view of the ICS with a detailed understanding of the system and its environment. The inventory measure can be considered as a mapping of multiple types: physical, logical, application, administration/Monitoring.

a: PHYSICAL MAP

The physical map is supposed to display geographic distributions of devices in different sites. It contains the following elements:

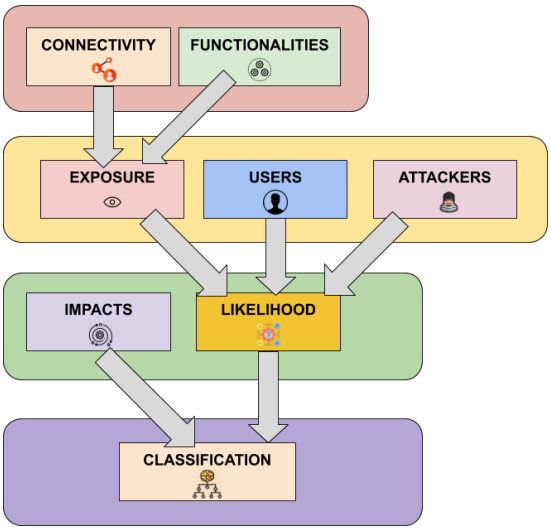

FIGURE 13. Risks classification flowchart.

- The list of communicating devices in the network and ICS (names, brand, model, etc.);
- Diagrams with geographical locations (switches, plant interconnections with MPLS).

b: LOGICAL MAP

The logical map is a topology of networks (IP scheme, subnet, links, main devices) with:

- List of organisations and related people responsible;
- List of IP address ranges (switches, interconnections);
- List of non-ip networks (mac addresses, switches, functional description);
- List of non-ethernet access points (ports, devices, protocols);
- List of logical servers (ip addressing, OS, business apps, services, etc.).

c: APPLICATION MAP

The application map focuses on business applications and their data streams. It should show the following items:

- Person responsible;
- Type of application (SCADA, PLC, etc.);
- Number of users;
- Devices;
- Listening services on the networks (ports);
- Application flows and version.

d: ADMINISTRATION/MONITORING MAP

The administration map is necessary only in the case of a centralized management of administrative rights, which is often the case in smart manufacturing. This map contains:

- Directories;
- Management infrastructures;
- Systems to manage logs, security events;
- Supervisory system (alarm, intrusion detection sensor);
- Active directory domains, forests, support servers;
- Relationships with external domains.

4) USER STRAINING AND CERTIFICATION

Users who work on an ICS should be trained to ensure system security. This training includes awareness about risks inherent to technologies. The training must be carried out by certified providers. Two actions are considered as directives. The first action imposes cybersecurity training and certification to all users. The second one establishes a conduct policy that must be signed by users upon arrival.

5) AUDITS

To ensure the security level does not degrade over time, cybersecurity tests and audits should be conducted regularly. The audit process should include the suppliers. In the industrial sector, two types of audit exist, which are the Site Acceptance Test (SAT) at vendor's test facility, and the Factory Acceptance Test (FAT) at client's site. These audits include the following components:

- Error testing about operational functions;
- Simulation of threat scenarios;
- Performance evaluation;
- Verification of security mechanisms.

6) BUSINESS RESUMPTION PLAN AND BUSINESS CONTINUITY PLAN

After an incident, whatever its origin, an organisation must guarantee its ability to resume its activity fast. To do that, it is mandatory to establish a Business Resumption Plan (BRP) or a Business Continuity Plan (BCP). These plans must include:

- Incident scenarios identified by risk analysis / vulnerability assessment;
- Back-up plan for sensitive data to enable ICS to be rebuilt after loss.

7) EMERGENCY/DEGRADED MODES

To enable rapid response to an incident, emergency procedures (also called degraded modes) must be established. The emergency modes must respect the following conditions:

- Do not constitute a degradation of cybersecurity level;
- Closely governed, so that they cannot be used as exploitable vulnerabilities;
- Enable installations to stop without causing damage;
- Continue to operate when directed in manual mode.

8) ALERT AND CRISIS MANAGEMENT PROCESS

The alert and crisis management process helps to establish procedures responding to incident scenarios identified by risk analysis. As a security process, it should be regularly tested to verify its effectiveness. It answers the following questions:

- What to do when an incident is detected;
- Who to alert;
- Who should coordinate the actions;
- Which initial measures to apply;
- Escalation procedure to decide about legal actions or BCP instigation;
- Post-incident analysis to determine the cause of the incident, and to improve cybersecurity.

9) THIRD PARTY MANAGEMENT

Third party access must also be considered in the smart manufacturing context, as it was pointed out by ENISA [47]. The following conditions must be respected:

- Strict access control with specific purpose, and with the least privilege necessary;
- No direct connection for the vendor to a system in control or production layer;
- Prompt suppliers about security of their processes;
- Clearly define relevant aspects of the partnership with third parties, including security, and mention them in the agreements and contracts.

E. TECHNICAL GOOD PRACTICES

After these steps (policies and organisational practices) related to formalization, security also needs to be addressed through appropriate technical capabilities and environments where they are deployed [47], [50]. The tables 8 and 9 summarize those practices proposed by ANSSI. For every practice, the following details are exposed:

- The reason why it should be considered;
- The method to apply it;
- Its scope (hardware, networks, infrastructure, etc.);
- Constraints related to its application;
- How to handle these constraints.

However, some measures related to IoT and smart manufacturing are missing, which is why they will be detailed in the following subsections.

1) TRUST AND INTEGRITY

This practice helps to ensure integrity and trustfulness of data and devices. The following measures must be applied:

- Verify software integrity and source before running it;
- For IoT devices, authorize them within the network by using digital certificates/PKI;
- Definition of secured data exchange channels for IoT devices (white list);
- Implementation of application white lists, and periodic (annual) review of the list in case of change;
- Utilisation of cryptography mechanisms to ensure production data integrity;
- Monitor data at rest and in transit to detect unauthorized modifications.

2) CLOUD SECURITY

Cloud computing security aspect is concerned by this practice. The following measures must be applied:

- Choice of the type of cloud based on business, privacy impact, laws, cloud provider's country;
- Inclusion of security and availability aspects in the agreements with cloud providers;
- Avoid single point of failure with cloud applications and centralized systems;

TABLE 8. Cybersecurity technical good practices for Industry 4.0 (1/2).

Practice	Reason	Method	Scope	Constraints	Constraint management
Control physical access points	Determine entry points in the system	Identify access (who? why? how often?), Protect access to servers, devices, cables (IT rooms, locked cabinets)	Workstations, servers, network devices, machines, touch screens	Size of system, maintain access even in case of emergency	Door "dry contact" with alarms, break glass procedures
Network segregation	Limit attack propagation and contain vulnerabilities	Establish flow map, filter, trace and separate network with VLANs	Networks (SCADA, PLC, development...)	Real-time constraints (process networks)	Filtering applied upstream, physical access control to network devices
Management of portable devices	Reduce malware attack risks through portable media (usb, hdd...)	Define policy, software restrictions, restrict use of this media, usb ports	Workstations, servers, consoles, touch screens	Data exchange between networks not connected	Clean machines (reinforced, secured) dedicated for data transfers
Account management	Protects from unauthorized access	Accounts policy (users/apps), no default credentials, strong passwords changed regularly	OS, databases, apps (SCADA/PLC), network devices, machines	Generic accounts, emergency access	Trace actions, strict procedures to determine identity with generic accounts (moment-by-moment)
Configuration hardening	Limit areas exposed to attacks	Install only necessary software, protocols and services, avoid default options, disable vulnerable protocols	OS, apps (SCADA/PLC), network devices, touch screens	Impact of modifications on production apps	Documented analysis, exception handling for unsecured functionalities needed
Monitoring, warnings and alarms	Detection of intrusions, tracing of actions, maintenance interventions	Activate traceability functions (syslog, windows events...), filter and generate alerts for relevant events	OS, databases, network devices, PLC...	High volume of logs generated	Tools for managing events (filter, limit, remove...)
Configuration management	Ensure there are no malicious modifications between versions	Comparison between apps executed and reference app configuration, identification of variations before deployment	Apps (SCADA/PLC), network devices (config files)	Complexity and heterogeneity of ICS	Configuration management tools to identify variations between two versions

- Determination of critical systems and applications when using public cloud;
- To reduce the risks of cloud attacks, use a zero-knowledge approach, and protect all data within cloud and during transfer.

3) MACHINE-TO-MACHINE SECURITY

The concept of Machine-to-Machine security is related to key storage, encryption, input validation and protection during machine-to-machine communications. The following measures must be applied:

- Usage of a server-HSM in the infrastructure to store long-term service-layer keys;
- Security association between communicating entities and cryptography algorithms to provide mutual authentication, integrity and confidentiality;
- Use of communication protocols able to detect unauthorized repeat of earlier messages;

TABLE 9. Cybersecurity technical good practices for Industry 4.0 (2/2).

Practice	Reason	Method	Scope	Constraints	Constraint management
Backup and restoration	Possess data in case of full restart after an attack or disaster	Backup policy (which data to backup for users or based on regulatory requirements ?)	Source codes, databases, histories, firmwares of PLCs, configs of network devices (switches, routers...)	Backup can't be done automatically for some devices (sensors, actuators for PLCs)	Trace modifications of settings, control, adjustment, alarms for sensors / actuators
Documentations	To have an exact representation of ICS and to control information dissemination	Documentation policy (update process, retention period, storage...)	Plant, architectural diagrams, locations, admin and maintenance manuals, system analysis...	Hard copies of documents can contain passwords (on-call staff), their control is complicated	Awareness of users regarding risks with documentation, no documents in view on desk...
Malicious code detection	Advance protection against virus attacks	Protection policy, priority to hardware / apps in direct contact with outside world and users	SCADA apps, engineering stations, programming and maintenance consoles	Incompatibility with older apps, no antivirus update, contractual issues (guarantee loss)	Deploy antivirus on portable and maintenance machines, configuration reinforcement
Upgrade and patch management	Preventive protection against attacks, failures associated with bugs, vulnerabilities	Management policy for patches (systematic or periodic) suited to constraints, risks and hardware identified	OS, apps, firmware, operator machines, servers, PLCs, telecom devices, touch screens...	Patches must be assessed before deployment, some devices not easy to stop	Identify vulnerabilities, plan updates, monitor traffic, harden configs and isolate devices
Protection of PLCs	Protection of PLC programmes	Protected access (passwords) to PLC, source code, read-only access for first level maintenance, lock PLC cabinets	Production PLC, PLC programmes	...	...
Engineering and development stations	Vulnerability points and contamination vectors (portable, connection to other networks)	Patches, antivirus softwares, no connection outside SCADA, usage monitoring, shutdown when not in use	SCADA development stations, PLC console, portable devices to configure sensors and actuators	...	...

- To protect against cross-site scripting and command injection, use white list input validation.

4) DATA PROTECTION

Data protection is a very general concept, but in this case, it is related to the ensuring of data confidentiality on various levels of an organisation, and data access management. The following measures must be applied:

- Protection of data at rest (volatile and non-volatile memory), in transit and in use.
- Categorization of data based on risk analysis, criticality assessment, and security measures definition.
- Grant access to certain data to third parties with least privilege, and document this access.
- For high confidentiality data, use encryption, key management and data loss prevention solutions.

- Secure and anonymize direct and indirect personal data processed through access controls, roles and encryption.

5) SOFTWARE/FIRMWARE UPDATES

Like any other device, software updates on IoT solutions must follow a specific methodology, which measures are:

- Ensure tight control over the update (no alteration between the source and the destination).
- Perform deployment of patches only after testing and proving that there are no negative consequences.
- For systems which cannot be updated, compensating measures must be applied.

6) ACCESS CONTROL

IoT devices are critical devices in Industry 4.0, and can be accessed remotely or physically. That is why the following access control measures should be applied:

- Minimum level of authentication and authorization for a certain segment of the system.
- Implementation of multi-factor authentication.
- Apply the least privilege principle.
- Implementation of an account lockout functionality.
- Segregation of remote access.
- Consideration of physical access security.

7) NETWORKS, PROTOCOLS AND ENCRYPTION

Proper protocol implementation, encryption and network segmentation are key elements to build a strong IoT network. The following measures are related to this objective:

- Use of secure communication channels and encryption when possible;
- Use proven-in-use protocols based on standards (TLS 1.3), and avoid vulnerable ones (Telnet, SNMP v1/v2);
- Limit the number of protocols within a given environment, and disable unused services.
- Ensure security capabilities and interoperability between the protocols.

8) MONITORING AND AUDITING

Several measures are suggested for IoT environment regarding network traffic, availability monitoring and log review:

- Implementation of a passive monitoring solution to create an industrial network traffic baseline;
- Analysis of security logs in real-time using SIEM (Security Information and Event Management) solutions;
- Periodic review of the logs, the access privileges and the configurations;
- Monitor availability of IoT devices in real time.

9) CONFIGURATION MANAGEMENT

IoT include a wide range of devices, it is important to keep a track of changes in configurations, device hardening and backup methods. The following measures allow that:

- Baseline security configurations tailored to different types of assets;
- Document any change in configuration according to change management policy of the organisation;
- Implementation of supporting tools which enable configuration management;
- Creation of a comprehensive backup plan, tailored to different types of assets.

VII. CONCLUSION

This paper has explored cybersecurity concepts and solutions within the Industry 4.0 context through the scientific and normative literature. In the analyzed papers, some aspects of cybersecurity were not always mentioned, such as the managerial aspect of cybersecurity or business impacts. For this reason, our study proposed was structured as a step-by-step approach to give a complete view of the topic. In addition to be an introductory review of scientific work regarding cybersecurity, it can also be used as a guide for presenting cybersecurity in smart manufacturing environment.

After introducing the Industry 4.0 concept, we showed the complexity induced by cybersecurity mechanisms to keep systems safe, due to numerous new technologies involved. We then proposed a characterization of cybersecurity with regard to both technical and managerial aspects to show that every level of an organisation has a role to play. Moreover, we pointed out that cybersecurity could also be a lever for value creation. Given that cybersecurity should be considered according to physical areas, we proposed a division of a factory into several perimeters, that we characterized based on their interactions, equipment, and networks. We then reported the cybersecurity vulnerabilities, threats and risks encountered in Industry 4.0 factories for each perimeter, while taking into account business impacts at organisational level.

A state of the art of recent cybersecurity solutions of the literature has been reported. They can be applied at physical or virtual levels, and they all try to anticipate the attacks, contrary to classical approaches where the cybersecurity response occured mainly after the attack. It should be noticed that, in addition to expert system paradigm usually implemented in cybersecurity solutions, new innovative technologies, such as machine learning, honeypots and digital twins, are used in the recent solutions. We completed this review of scientific solutions by a state of the art of the guidelines promoted by official organisations such as ISO, ENISA, ANSSI, NIST, and that can be used as a starting point to establish a cybersecurity strategy. Through the analysis conducted in this paper, it is clear that cybersecurity is not just a technical concern. Any cybersecurity solution needs support from multiple actors to be included in the comprehensive strategy of an Industry 4.0 factory, and all users need to be trained and made aware of cybersecurity risks.

APPENDIX A

See Table 10.

APPENDIX B ATTRIBUTION

The icons used in figures come from https://flaticon.com

TABLE 10. Abbreviations.

Terms	Definitions
ANSSI	French national cybersecurity agency
APT	Advanced Persistent Threats
BCP	Business Continuity Plan
BRP	Business Resumption Plan
CIM	Computer Integrated Manufacturing
CIS	Computational Intelligence System
CPS	Cyber Physical System
C-Suite	Chief Suite
DCS	Distributed Control System
DNP	Distributed Network Protocol
DoS	Denial of Service
EIF	Ensemble Intelligence Framework
ENISA	European Network Information Security Agency
FAT	Factory Acceptance Test
GA	Genetic Algorithm
GDPR	General Data Protection Regulation
HMI	Human Machine Interface
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IoT	Internet of Things
IPS	Intrusion Prevention System
IS	Information System
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
IT	Information Technology
MDSEA	Model-Driven Service Engineering Architecture
MES	Manufacturing Execution System
MPLS	Multi-Protocol Label Switching
MSED	Manufacturing Security Enforcement Device
NIST	National Institute of Standards and Technology
NNO	Neural Network Oracle
OPC UA	Open Platform Communication Unified Architecture
OS	Operating System
OT	Operation Technology
PIA	Privacy Impact Analysis
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SAT	Site Acceptance Test
SCADA	Supervisory Control And Data Acquisition
SDCM	Software Defined Cloud Manufacturing
SDN	Software Defined Networking
SIEM	Security Information and Event Management
SPIT	Spam over Internet Technology
VM	Virtual Machine

REFERENCES

[1] H. Kagermann, W. Wahlster, and J. Helbig, "Recommendations for implementing the strategic initiative industrie 4.0—Securing the future of German manufacturing industry," Nat. Acad. Sci. Eng., Industrie 4.0 Working Group, München, Germany, Tech. Rep., Apr. 2013. [Online]. Available: https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf

[2] O. Cohin and P. Sondi, "Internet of Things for smart factory," *IEEE COMSOC MMTC E-Lett.*, vol. 10, no. 5, pp. 21–23, Sep. 2015.

[3] V. Alcácer and V. Cruz-Machado, "Scanning the industry 4.0: A literature review on technologies for manufacturing systems," *Eng. Sci. Technol., Int. J.*, vol. 22, no. 3, pp. 899–919, Jun. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2215098618317750

[4] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45201–45218, 2019.

[5] M. Dawson, "Cyber security in industry 4.0: The pitfalls of having hyperconnected systems," *J. Strategic Manage. Stud.*, vol. 10, no. 1, pp. 19–28, 2018.

[6] J. Prinsloo, S. Sinha, and B. von Solms, "A review of industry 4.0 manufacturing process security risks," *Appl. Sci.*, vol. 9, no. 23, p. 5105, Nov. 2019.

[7] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101677. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404819302172

[8] A. Angelopoulos, E. T. Michailidis, N. Nomikos, P. Trakadas, A. Hatziefremidis, S. Voliotis, and T. Zahariadis, "Tackling faults in the industry 4.0 era—A survey of machine-learning solutions and key aspects," *Sensors*, vol. 20, no. 1, p. 109, Dec. 2019, doi: 10.3390/s20010109.

[9] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2489–2520, 4th Quart., 2020.

[10] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for industry 4.0 in the current literature: A reference framework," *Comput. Ind.*, vol. 103, pp. 97–110, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0166361518303658

[11] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, "Addressing industry 4.0 cybersecurity challenges," *IEEE Eng. Manag. Rev.*, vol. 47, no. 3, pp. 79–86, Sep. 2019.

[12] X. T. Nguyen and Q. K. Luu, "Factors affecting adoption of industry 4.0 by small- and medium-sized enterprises: A case in Ho Chi Minh City, Vietnam," *J. Asian Finance, Econ. Bus.*, vol. 7, no. 6, pp. 255–264, Jun. 2020.

[13] F. Sicard, É. Zamai, and J.-M. Flaus, "An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems," *Rel. Eng. Syst. Saf.*, vol. 188, pp. 584–603, Aug. 2019.

[14] J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, "Current cyber-defense trends in industrial control systems," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101561.

[15] M. R. Asghar, Q. Hu, and S. Zeadally, "Cybersecurity in industrial control systems: Issues, technologies, and challenges," *Comput. Netw.*, vol. 165, Dec. 2019, Art. no. 106946.

[16] T. Lu, X. Guo, Y. Li, Y. Peng, X. Zhang, F. Xie, and Y. Gao, "Cyberphysical security for industrial control systems based on wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 6, Jun. 2014, Art. no. 438350, doi: 10.1155/2014/438350.

[17] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things and industry 4.0," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 17–27, Mar. 2017.

[18] F. Bonavolontà, A. Tedesco, R. S. L. Moriello, and A. Tufano, "Enabling wireless technologies for industry 4.0: State of the art," in *Proc. IEEE Int. Workshop Meas. Netw. (M&N)*, Sep. 2017, pp. 1–5.

[19] J. Villain, V. Deniau, A. Fleury, C. Gransart, and E. P. Simon, "Detection of cyber-attacks on Wi-Fi networks by classification of spectral data," in *Proc. 33rd Gen. Assem. Sci. Symp. Int. Union Radio Sci.*, Aug. 2020, pp. 1–3.

[20] T. Pereira, L. Barreto, and A. Amaral, "Network and information security challenges within industry 4.0 paradigm," *Procedia Manuf.*, vol. 13, pp. 1253–1260, Jun. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2351978917306820

[21] M. Alani and M. Alloghani, *Security Challenges in the Industry 4.0 Era*. Cham, Switzerland: Springer, Apr. 2019.

[22] M. Kiss, G. Breda, and L. Muha, "Information security aspects of industry 4.0," *Procedia Manuf.*, vol. 32, pp. 848–855, Jan. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2351978919303294

[23] A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Comput. Ind.*, vol. 114, Jan. 2020, Art. no. 103165.

[24] A. Kondiloglu, H. Bayer, E. Celik, and M. Atalay, "Information security breaches and precautions on industry 4.0," *Tehnologičnij Audit ta Rezervi Virobnictva*, vol. 6, no. 4, pp. 58–63, 2017. [Online]. Available: https://doaj.org/article/fed113013c484cdc8f3ac0898592b152

[25] Z. Illési, A. Halász, and P. J. Varga, "Wireless networks and critical information infrastructure," in *Proc. IEEE 12th Int. Symp. Appl. Comput. Intell. Informat. (SACI)*, May 2018, pp. 000255–000260.

[26] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1617–1634, 3rd Quart., 2014.

[27] D. Satasiya and R. Rupal D., "Analysis of software defined network firewall (SDF)," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2016, pp. 228–231.

[28] P. Zeng, Z. Wang, Z. Jia, L. Kong, D. Li, and X. Jin, "Time-slotted software-defined industrial Ethernet for real-time quality of service in industry 4.0," *Future Gener. Comput. Syst.*, vol. 99, pp. 1–10, Oct. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X18311427

[29] A. Tsuchiya, F. Fraile, I. Koshijima, A. Ortiz, and R. Poler, "Software defined networking firewall for industry 4.0 manufacturing systems," *J. Ind. Eng. Manage.*, vol. 11, no. 2, pp. 318–333, 2018. [Online]. Available: https://doaj.org/article/47009ec439bb438b8c71985fa939e74f

[30] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[31] M. Wolf and D. Serpanos, "Safety and security in cyber-physical systems and Internet-of-Things systems," *Proc. IEEE*, vol. 106, no. 1, pp. 9–20, Jan. 2018.

[32] B. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins, and R. Jardim-Goncalves, "An ontology-based cybersecurity framework for the Internet of Things," *Sensors*, vol. 18, no. 9, p. 3053, Sep. 2018. [Online]. Available: https://doaj.org/article/2efde4be22aa4f5aadf569bdbe58d62f

[33] B. A. Mozzaquatro, R. Jardim-Goncalves, and C. Agostinho, "Towards a reference ontology for security in the Internet of Things," in *Proc. IEEE Int. Workshop Meas. Netw.*, Oct. 2015, pp. 1–6.

[34] A. Wegner, J. Graham, and E. Ribble, *A New Approach to Cyberphysical Security in Industry 4.0*. Cham, Switzerland: Springer, 2017, pp. 59–72, doi: 10.1007/978-3-319-50660-9_3.

[35] Y. Pan, J. White, D. Schmidt, A. Elhabashy, L. Sturm, J. Camelio, and C. Williams, "Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems," *Int. J. Interact. Multimedia Artif. Intell.*, vol. 4, pp. 45–54, Mar. 2017.

[36] J. Graham, J. Hieb, and J. Naber, "Improving cybersecurity for industrial control systems," in *Proc. IEEE 25th Int. Symp. Ind. Electron. (ISIE)*, Jun. 2016, pp. 618–623.

[37] L. Thames and D. Schaefer, *Cybersecurity for Industry 4.0 and Advanced Manufacturing Environments With Ensemble Intelligence*. Cham, Switzerland: Springer, 2017, pp. 243–265, doi: 10.1007/978-3-319-50660-9_10.

[38] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Appl. Sci.*, vol. 9, no. 20, p. 4396, Oct. 2019.

[39] G. Zhao, C. Zhang, and L. Zheng, "Intrusion detection using deep belief network and probabilistic neural network," in *Proc. IEEE Int. Conf. Comput. Sci. Eng. (CSE), IEEE Int. Conf. Embedded Ubiquitous Comput. (EUC)*, vol. 1, Jul. 2017, pp. 639–642.

[40] F. Sicard, E. Zamai, and J.-M. Flaus, *Critical States Distance Filter Based Approach for Detection and Blockage of Cyberattacks in Industrial Control Systems*. Cham, Switzerland: Springer, 2018, pp. 117–145, doi: 10.1007/978-3-319-74962-4_5.

[41] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, May 2016.

[42] R. Mitchell and I.-R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1254–1263, Sep. 2013.

[43] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in SCADA systems," *IEEE Trans. Ind. Informat.*, vol. 7, no. 2, pp. 179–186, May 2011.

[44] S. Petrenko, *Developing a Cybersecurity Immune System for Industry 4.0*. Gistrup, Denmark: River Publishers, 2020, pp. 1–116.

[45] M. Eckhart and A. Ekelhart, *Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook*. Cham, Switzerland: Springer, Dec. 2019, pp. 383–412.

[46] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Apr. 2018, doi: 10.6028/nist.cswp.04162018.

[47] ENISA. (Nov. 2018). *Good Practices for Security of Internet of Things in the Context of Smart Manufacturing*. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport

[48] ANSSI. (2014). *Cybersecurity for Industrial Control Systems: Classification Method and Key Measures*. [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf

[49] ANSSI. (2014). *Cybersecurity for Industrial Control Systems: Detailed Measures*. [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_detailed_measures.pdf

[50] ANSSI. (2014). *Managing Cybersecurity for Industrial Control Systems*. [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/01/Managing_Cybe_for_ICS_EN.pdf

VALENTIN MULLET received the master's degree in computer science from the University of Littoral Côte d'Opale, in 2018, where he is currently pursuing the Ph.D. degree with the Laboratory of Informatics, Signal and Image of the Cote d'Opale (LISIC), University of Littoral Côte d'Opale. His areas of interest include the Internet of Things, cybersecurity, traceability, data management, and blockchain applications in manufacturing factories in the context of industry 4.0.

PATRICK SONDI received the Ph.D. degree in computer science from the University of Valenciennes, in 2010. He joined the University of Littoral and Côte d'Opale as an Associate Professor, in 2013. His research interests include protocol engineering, quality of service, safety, security and event-based simulation of wired and wireless networks, especially their application in industrial and transportation systems.

ERIC RAMAT received the Ph.D. degree in computer science from the University of Tours, in 1997. He joined the University of Littoral and Côte d'Opale as an Associate Professor in 1998 and as a Professor in 2004. His research interests include complex system modeling, multi-modeling, heterogeneous model coupling, DEVS formalism, and their extensions and discrete event simulation.