1

Challenges Involving Cybersecurity and Traceability in Factory 4.0

1.1. Introduction

The industrial sector has witnessed several revolutions over the last few centuries (Figure 1.1). The first occurred with mechanization, introduced by the steam engine, in 1765. Driven by electricity and oil production in 1870, mass production brought about the second revolution through the development of high-tech industries such as automobiles and aeronautics. The third revolution was that of automated production in 1969, supported by electronics with the advent of the transistor and the microprocessor; it subsequently initiated the appearance of programmable logic controllers (PLCs), robots and computer technologies in factories.

In 2011, a fourth phase was conceptualized in Germany as an evolution of traditional factories (Kagermann et al. 2013) toward more flexibility and adaptation to constantly developing production environments: the Industry 4.0 paradigm, also known as the Industrial Internet of Things (IoT) or Industrial Internet, was born. For example, in the agri-food sector, the goal of the Industry 4.0 paradigm is to connect farms and product processing plants to the Internet in order to improve overall efficiency and productivity (approximately 15%–20% targeted).

On a more general level, the necessary hyperconnectivity for this operation must allow the collection of large volumes of data originating from the value chain to be used for a wide range of purposes, such as:

For a color version of all the figures in this chapter, see: www.iste.co.uk/sondimullet/cybersecurity.zip

Cybersecurity and Traceability in Factory 4.0,
coordinated by Patrick SONDI and Valentin MULLET. © ISTE Ltd 2026.

– exchange of information in real time between devices belonging to factories, suppliers or customers;

– data acquisition and storage for traceability and computing performance management;

– data processing for predictive maintenance or remote monitoring to reduce machine downtime;

– task automation and stock reduction;

– improved service levels and product quality.

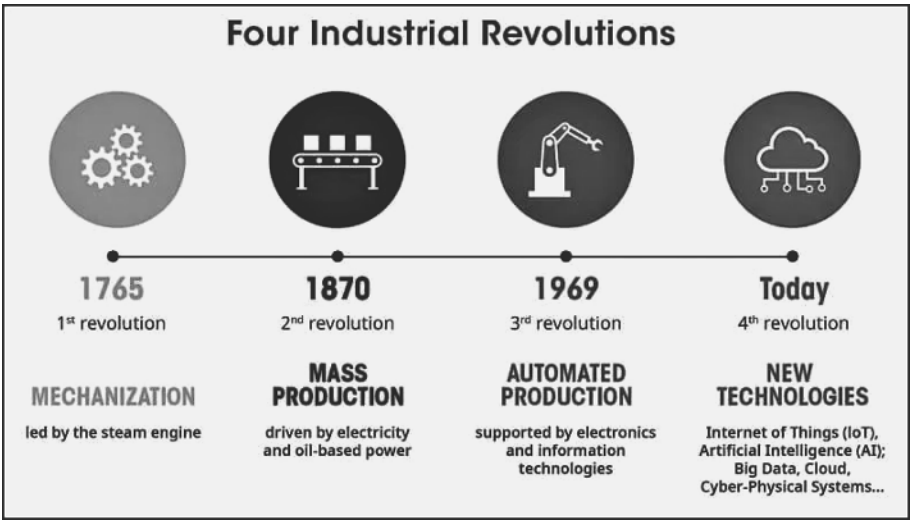

Figure 1.1. *Timeline of the industrial revolutions (source: Geandarme 2018)*

The implementation of Industry 4.0 consists on the one hand of collecting as much information as possible about industrial activity in order to digitize it, process it and aggregate it with other information. This digital transformation or digitalization is materialized by the introduction in the factory of innovative technological objects such as the IoT, especially for collecting data and industrial control, Cloud computing for the processing and storage of these massive amounts of data (Big Data) and optimization tools using artificial intelligence (AI) for the automation of factory management. However, it brings about several drawbacks that are imported in parallel into the industrial activity, namely problems inherent in new technologies in terms of operational safety and cybersecurity, as well as the creation of new dependencies likely to undermine the resilience of industrial activity itself. Nevertheless, these technological objects are necessary to connect operators and

machines or equipment with production management tools in order to adapt to customer requests and provide a quick response to the slightest variation. Factory 4.0 can thus achieve a high level of control customization in a context that mainly remains that of mass production. As such, innovative objects are involved in the creation of a significant part of the value and in improving the quality and standards of the factory, de facto justifying their adoption.

On the other hand, working in Factory 4.0 is perceived differently due to the implementation of combined processes between machines and operators. The global challenges of developing Industry 4.0 therefore also include, in addition to the technical means themselves, equipment and training specifically oriented for operators in connection with new technologies. As an example, we can mention all the developments in augmented reality (AR) and virtual reality (VR) that allow new forms of interaction between the operator, the production system and the control system. These aspects are an integral part of a fifth stage of the evolution of the industry initiated by the European Union (European Commission 2021) referred to as Industry 5.0 but will not be specifically addressed in this book. They highlight however that the development of the industry of the future requires a balanced distribution of resources between operator training, investment in equipment and data protection.

1.2. Traceability challenges in Factory 4.0

Consequently, although the central subject of this book is traceability in Industry 4.0, the hyperconnectivity that characterizes this context implies that this traceability be outlined and addressed in conjunction with their relationship to cybersecurity.

Considered for a long time a response to regulatory and commercial constraints or even a marginal resource in technical diagnostics, traceability has become a driver for performance improvement within the context of the digital transformation of factories. The new technologies of Industry 4.0 are actually based on the use of collected and historical data, of which a significant part is created by industrial traceability. With the increasing digitization of industry, traceability is now part of all production units within a factory. All stages, from design to delivery, including production processes, are involved in data collection, processing and analysis.

1.2.1. *The volume of data*

Nonetheless, this generalization causes the volumes of data generated by traceability processes to often exceed the storage capacities of a factory. In a report

published in 2018 (Reinsel et al. 2018), IDC (International Data Corporation), in partnership with Seagate, proposed in its white paper a study comparing the amount of data (called "the datasphere") generated by different professional sectors (Figure 1.2). The share of the manufacturing industry is the largest with 3584 Eo (10^{18} bytes) due to its maturity, the industry's investment in the IoT and its ability to produce 24 hours a day and 7 days a week.

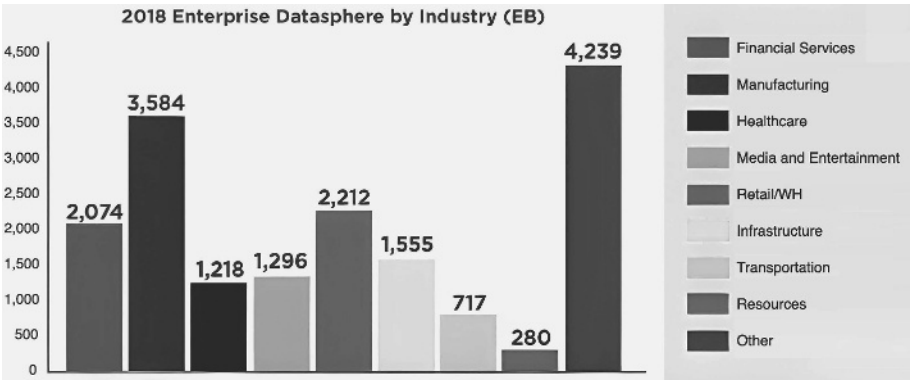

Figure 1.2. *Datasphere of companies classified by industry (source: Reinsel et al. 2018)*

To address this problem, plant managers are resorting to outsourcing the storage of their data to the Cloud. This presents several major risks such as Internet dependency, exposure of the factory IT system to the Internet, loss of control over data access management and even geopolitical risks. It is therefore necessary that the management of this problem of data volume be addressed in a more global context including cybersecurity considerations.

1.2.2. *Transparency*

For companies, the supply chain is a fundamental area that consists of tracking the origin and history of products from beginning to end. However, its opacity and lack of data recording were seen as major issues. This opacity was due in part to the obsolescence of the system, which was still too often based on paper-based registers requiring manual handling that therefore was prone to errors, loss of time and loss of information because of its volatility. The digitalization of traceability introduced by Industry 4.0 provides, in part, a solution to this problem.

Product quality and origin are indicators whose importance is emphasized by companies as guarantees of brand image and meeting customer needs. Given that

the need for visibility is thus more pressing, companies are compelled to improve the transparency and traceability of their supply chain. In this context, the notion of transparency focuses on mapping the entire supply chain and traceability examines individual batches of components or purchase orders as they progress through the supply chain. Another question of vigilance for these companies is the fight against counterfeiting, which finds in this system of total traceability an effective tool to guarantee product authenticity. In this regard, traceability represents an investigation tool for identifying what causes defects in products or inefficiencies in production processes. When it includes several actors of the supply chain, in particular suppliers, customers, regulators and other potential auditors, data integrity and open access must be guaranteed to each actor under well-defined conditions.

The organization of the traceability system for ensuring this transparency, in addition to integrity and open access to data, has many implications on factory cybersecurity. In addition, the need for transparency should not be satisfied at the expense of another aspect, which is confidentiality. Indeed, data generated by production processes may contain critical information relating to the know-how or other crucial interests of the factory and which cannot therefore be exposed at the risk of jeopardizing the company's competitiveness. This is all the more critical as the volume of data is almost systematically the main factor for resorting to the use of Cloud computing for the storage of at least part of it. A balance must therefore be found, in connection with cybersecurity, in order to be able to guarantee transparency, integrity and compliance with confidentiality within the traceability system for the data to which it applies.

1.2.3. *The contribution of blockchain*

Blockchain is one of the components of Industry 4.0 and it provides a set of functionalities that enables the implementation of a historical data register while guaranteeing transparency, integrity and free access to participants. Part of the work presented in this book consists of adding mechanisms that guarantee confidentiality to the data that requires it. In this case, the aim of the research covered throughout this book is to reach the following objectives:

1) develop the conventional factory traceability system toward the blockchain by covering the supply chain, from the supplier up to the customer;

2) guarantee the integrity, transparency and confidentiality of critical data within this system;

3) achieve a successful assessment of the impacts of this evolution from the traceability system to the blockchain by means of a simulation tool that could also be used as a tool for evaluations prior to development planning.

Nevertheless, for a better understanding of the issues related to the implementation of this blockchain-based traceability, as well as its outlines relating to the cybersecurity of a factory 4.0, we will first present a generic description framework for a factory, as well as a description of cybersecurity based on this framework (Mullet et al. 2021). The studies concerning traceability and its implementation using a blockchain will be the subject of the following chapters.

1.3. Plant overview

In order to better understand the notion of cybersecurity within an industrial environment, it should be recalled that the factory comprises several departments with different requirements and work processes. We first propose a subdivision of the plant into six generic zones that we call perimeters.

1.3.1. *Definition of perimeters*

1.3.1.1. *Manufacturing production*

This is the main zone of a factory where the production lines are located, each allocated to some of the many stages required to manufacture final products. The devices existing in this perimeter belong to two groups: Industrial Control Systems (ICSs) and Cyber-Physical Systems (CPSs).

The ICS category mainly encompasses control components that act together to achieve an industry goal (Lezzi et al. 2018). These systems have been in use since the second half of the 20th century (Sicard et al. 2019). Within this category, we can mention the Programmable Logic Controller (PLC), the Remote Terminal Unit (RTU) and the Intelligent Electronic Device (IED) (Rubio et al. 2019). To interact with the hardware controller and access the data collected by the ICS environment, administrators utilize a Human–Machine Interface (HMI), which is also employed to display the device status (Asghar et al. 2019).

The second group, CPSs, is an umbrella for anything that integrates computing operations, networking or physical processes. These systems enable interaction between the digital world and the physical world. As an example, a manufacturing line can be thought of as a CPS (Lezzi et al. 2018). This is because they use sensors and other embedded systems to collect data from physical processes. Several authors (Lu et al. 2014; Lezzi et al. 2018) show that ICSs are a field of application for CPSs.

1.3.1.2. *Logistics zones*

Industrial logistics differs from traditional logistics in that it is adapted to the management of production flows, thus widening its field of action. Its perimeter

consists of multiple structures such as workshops and warehouses where forklifts are used. In this field where mobility is a key point, the devices used most are wireless devices (barcode scanners and tablets).

1.3.1.3. *Active supervision*

Active supervision represents tertiary activity, which covers the factory offices. It includes departments such as accounting, sales, human resources (HR) and the local IT system (IT). The most common devices are desktops, smartphones, monitors and printers.

1.3.1.4. *Research and development*

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

1.3.1.5. *Living zones*

The living zone corresponds to the rooms where employees gather (canteen, meeting rooms, rest rooms, etc.). These zones come with VoIP phones, tablets, screens, etc.

1.3.1.6. *External zones*

The external zone refers to everything located outside the factory. This includes physical places such as parking lots, as well as virtual places such as the Internet (Cloud, etc.).

1.3.2. *Interactions between perimeters*

The perimeters play a critical role in the industrial manufacturing process and their interaction at the IS level is mandatory, as can be seen in Table 1.1.

1.3.3. *Network perimeters in the factory*

Several types of ICSss can be found in the manufacturing sector (Asghar et al. 2019). These ICSs are categorized into two layers: the physical control layer and the logical control layer. This perimeter includes three subnetworks: the Supervisory Control And Data Acquisition (SCADA) system, Distributed Control Systems (DCSs) and programable logic controllers/sensors/protocols. Figure 1.3 depicts these different networks with the equipment and communication protocols used.

	Presence of computer interactions					
	Manufacturing-production	**Logistics**	**Active supervision**	**Research and development**	**Living area**	**External area**
Manufacturing-production	X	X	X	X		
Logistics	X	X	X	X	X	
Active supervision	X	X	X	X	X	X
Research and development	X		X	X		
Living areas			X		X	X
External areas			X		X	X

Table 1.1. *IT interactions between plant perimeters*

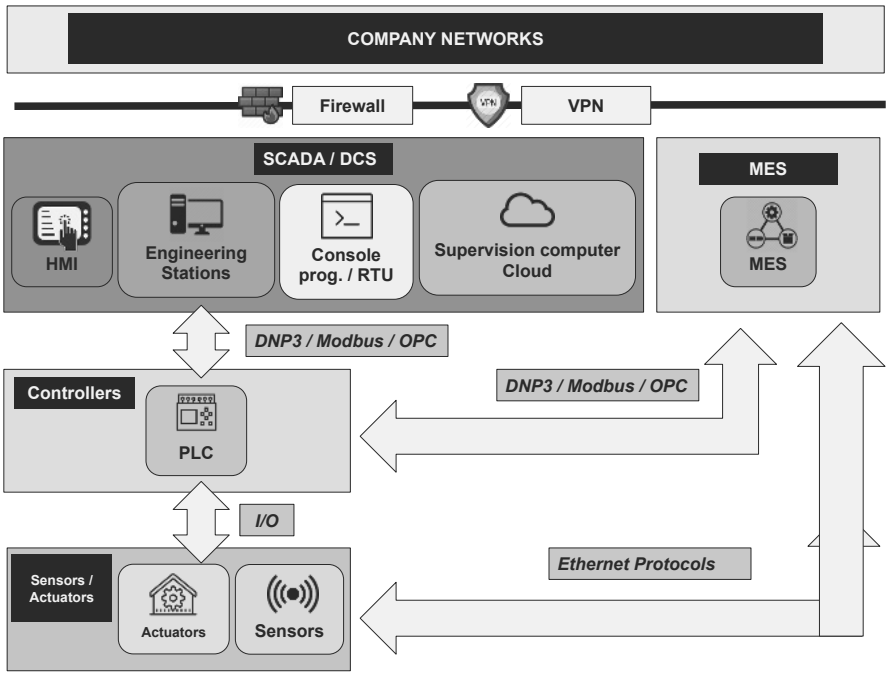

Figure 1.3. *Overview of the manufacturing-production perimeter networks*

1.3.3.1. *SCADA*

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

1.3.3.2. *DCS*

A DCS is composed of autonomous controllers installed in a manufacturing or production unit. The DCS system uses these controllers to remotely supervise and monitor a unit. The difference between DCS and SCADA systems is that the SCADA is adapted to individual site control due to its centralized nature, while DCSs can control complex processes that can span multiple sites because of its distributed network characteristics.

1.3.3.3. *PLC/sensors/protocols*

All control devices such as PLCs, sensors or protocols (DNP3/Modbus distributed network protocols) are located in the latter subnet, which is integrated into the physical control layer.

A PLC is the logical interface between SCADA and DCS systems. The PLC is designed to receive control commands and send back the status of the sensors. To establish the connection between the PLC and the SCADA (Abu Jassar et al. 2022), specific communication protocols have been designed by industrial system manufacturers (DNP3/Modbus/OPC).

1.3.4. *Access controls and perimeter monitoring*

From the moment interactions take place between perimeters, precise access controls have to be performed according to the information exchanged, which can be very sensitive. Another important aspect of security is monitoring, which allows users to be notified when a security breach occurs or when the system is under attack. Table 1.2 shows the different types of access controls available in the literature for the defined perimeters, as well as some monitoring solutions applicable to manufacturing plants.

1.4. Overview of cybersecurity in Industry 4.0

Industry 4.0 represents a revolution in the industrial world through the introduction of disruptive technologies such as the IoT and cloud computing within the factory. The resulting increased automation and improved production synergy between stock, supply chains and customer demands are accompanied by threats and attacks originating from the Internet. Despite the extensive literature existing on the topic of cybersecurity, many industrial players are only just beginning to realize the impact of cybersecurity on the preservation of their business. This part of the book will be dedicated to the presentation of the concepts and practical aspects related to the cybersecurity in an Industry 4.0 manufacturing plant. It focuses on the aspects of

cybersecurity related to traceability, but additional understanding can be gained by reading Flaus (2019).

In order to create this intelligent production environment, innovative technologies are needed to manage autonomous communications between every industrial device in the factory and the Internet. These technologies (Alcácer and Cruz-Machado 2019) include the IoT, cloud computing, big data, digital twins, AR, 3D printing, AI and new generation CPSs, as illustrated in Figure 1.4.

Plant perimeters	Equipment used	Access methods	Monitoring methods	Types of networks
Manufacturing-production	PLC, RTU, IED, HMI	Username/Password or badge access (human), Device ID via public and private keys (machines)	Video surveillance, traceability verification, logging, remote administration (SNMP or integrated)	SCADA, DCS
Logistics	Mobile terminals (tablets, barcode scanners, laptops)	Badge access (for humans), public/private keys (machines)	Video surveillance, system information control, logging, remote administration (IDS/IPS probes)	Wireless
Active supervision	Office automation, printers, laptops, smartphones	Password, badge access (human), network or system identification (terminals)	System controls, logging, remote administration (SNMP)	Office
Research and development	Workstations, experimental devices	Badge or biometric access (human), network	System verifications (terminals) and system checks, logging, remote administration (SNMP)	LAB
Living areas	VoIP telephony, wireless displays, tablets	No specific control (human), system information control (terminals)	Video surveillance, remote administration (SNMP or *built-in*)	Office
Physical external areas	Cameras	Badge access (human), system and network controls (terminals)	Logging, video surveillance, remote administration (SNMP, etc.)	CAM
Virtual external zones	Cloud service providers	ID/password (human), system and rules, firewalls (devices)	Logging, traffic monitoring, intrusion prevention (IPS) or detection system (IDS) probes	Internet

Table 1.2. *Factory perimeters in Industry 4.0*

In addition, Industry 4.0 promotes the application of these technologies to enable distributed communication architectures, such as Peer-to-Peer (P2P), instead of solely relying on standard cloud solutions or other centralized architectures.

The integration of these heterogeneous devices into the industrial cyber environment implies that cybersecurity has to be accounted for as part of the design strategy of companies wishing to implement the Industry 4.0 paradigm. Despite the

many improvements brought about by this revolution to the efficiency of manufacturing plants, flaws in cybersecurity can lead to critical impacts on the business model and a loss of competitiveness (Dawson 2018).

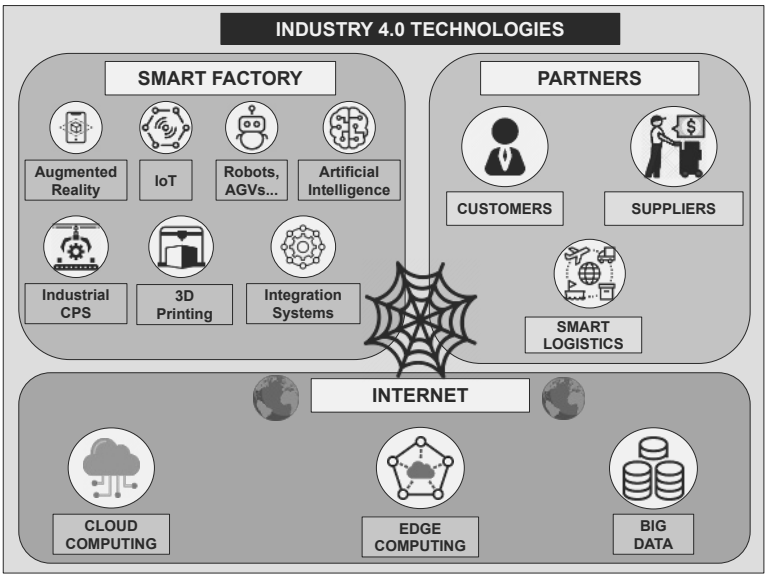

Figure 1.4. *Industry 4.0 technologies*

Several surveys show that only 16% of companies are willing to address the challenges of cybersecurity (Lezzi et al. 2018). The reasons provided include the lack of precise reference standards and the lack of managerial and technical skills to understand and implement them. Several organizations working on guidelines and standards help companies understand what schema they should use to reinforce their security and make it compliant. Among these organizations, to name a few, we can find: ANSSI (National Agency for the Security of Information Systems) in France, ENISA (European Union Agency for Cybersecurity) in the European Union and NIST (National Institute of Standards and Technology) in the United States.

A more detailed description of Industry 4.0 concepts and applications is provided in Prinsloo et al. (2019), as well as some recent cybersecurity attacks observed in several manufacturing plants around the world. The authors also propose countermeasures to address a wide range of cybersecurity risks. These risks must first be identified, along with the factors that cause them (Shukla et al. 2022). Another study proposed in Bhamare et al. (2020) focuses on cybersecurity, where the authors analyze in particular the transition from an ICSs in an autonomous factory to a

cloud-based environment, resorting to machine learning solutions. A more specific recent survey (Tange et al. 2020) reviewed 262 articles covering all aspects of Industry 4.0 security. In addition to a systematic review of the literature, their main proposals focus on the opportunities offered by fog computing in this field. All of these references are classic surveys that aim to provide the reader with a comprehensive overview of the literature.

1.5. Vulnerabilities, risks and threats in Industry 4.0

Industry 4.0 factories exhibit security vulnerabilities, like most organizational systems. The interconnection between devices makes security more complex and introduces unexpected vulnerabilities (Pereira et al. 2017; Alani and Alloghani 2019). In the industrial sector, manufacturing is the most targeted area by security attacks, and the number of threats is increasing every year (Lezzi et al. 2018).

Section 1.5.1 will focus on defining and describing vulnerabilities, threats and risks. Additional useful content and references can be found in Alqudhaibi et al. (2025).

1.5.1. *Definitions*

1.5.1.1. *Vulnerabilities*

In the computer field, vulnerabilities are defined by Lezzi et al. (2018) as weaknesses that could be exploited by hackers to compromise the system. More specifically, these weaknesses may be found in the system, in security procedures, or in internal controls. They can be classified into three categories which are remote access vulnerabilities, software vulnerabilities and Local Area Network (LAN) or Wireless LAN (WLAN) vulnerabilities.

1.5.1.2. *Threats*

A cybersecurity threat (also known as a cyber threat) is defined by Lezzi et al. (2018) as any circumstance impacting organizational operations, assets, individuals, other organizations or the nation by means of an information system through unauthorized access, destruction, disclosure or modification of information. Several parameters should be considered to analyze a cyber threat:

– the origin of the attack (internal or external);

– the goal;

– the affected cyber layer, including the runtime layer (sensors, actuators), the data transport layer (network) and the application layer (user data storage).

Within the framework of Industry 4.0, the following main cyber threat categories have been identified (Lezzi et al. 2018) to name but a few:

– direct attacks on external access;

– indirect attacks with a service provider to which external access has been provided;

– unknown attack vectors (or "zero-day exploits");

– malware;

– intrusion into neighboring networks.

1.5.1.3. *Risks*

According to Lezzi et al. (2018), a risk is the level of impact on organizational operations, assets or individuals resulting from the potential consequence of a threat and its likelihood of occurrence. In cybersecurity, risks are identified by the loss of certain characteristics such as availability, integrity, confidentiality and authentication.

1.5.1.3.1. Availability

The goal of availability attacks is to render the system unable to perform its usual tasks by overloading it. Their target can be equipment or access to the associated network by disrupting it. The most common types are Distributed Denial-of-Service (DDoS) attacks, which attempt to saturate the bandwidth or other resources in a system, making it unable to respond. Some attacks also affect the network, and more specifically routing operations ("gray hole", "black hole" and relay attacks).

1.5.1.3.2. Integrity

Integrity consists of maintaining data accuracy and completeness. The associated threats are similar to sabotage. They can be used to modify industrial communication protocols or network traffic. A major problem is that most of these protocols are inherited, which underlines the fact that no security considerations were involved during their design.

Some examples of common integrity attacks are "Man-In-the-Middle" attacks, which consists of tampering with and relaying communications between two entities, although these keep on operating as if they were directly connected.

1.5.1.3.3. Confidentiality

Confidentiality threats involve accessing or stealing sensitive data related to industrial processes, configurations, customers or administration. They can be categorized as cyber espionage and carried out in different environments or contexts such as passive network traffic analysis, active code injection into operational applications to obtain security credentials or corruption of control measures.

1.5.1.3.4. Authentication

This includes threats that take advantage of design flaws or software vulnerabilities to obtain privilege elevation and gain access to protected resources. These attacks make use of social engineering techniques such as phishing or spam chains to capture strategic information. Misconfigurations resulting in improper access at both the physical and logical levels can lead to the same security issues.

1.5.2. *Business impacts*

Cybersecurity threats are a serious topic, and they undermine the capabilities of the most advanced companies. A particularly critical year was 2017 as three large-scale attacks were carried out around the world (Kiss et al. 2019):

– "NotPetya" propagated to 65 countries and caused $892 million in damage.

– "Bad Rabbit" targeted critical infrastructure.

– "WannaCry" propagated to 150 countries and caused $8 billion in damage.

As a result, companies infected by these attacks saw their production interrupted for a long time and were not able to efficiently carry out their activities. The impact of these threats is not only technical or financial. It can affect relationships between partners and lead to legal consequences. Table 1.3 describes the analysis found in Corallo et al. (2020) on business impacts filtered by risks. All risks are covered by a range of threats and it is clearly visible that the number of impacts on companies is greater than the number of threats. Each unique threat incurs several business impacts, suggesting that no threat should be underestimated and that policies in terms of cybersecurity investments are needed (Sawik 2020).

1.5.3. *Major cybersecurity threats in Industry 4.0*

The main security threats facing an Industry 4.0 factory can be classified into the following categories (Pereira et al. 2017).

1.5.3.1. *Cyber espionage*

Due to intelligent and connected business processes, Industry 4.0 is vulnerable to cyber espionage. Well-organized cybercriminal groups have turned Industry 4.0 into their favorite playground to steal sensitive information and intellectual property. One such group is the Black Vine group, which primarily targets the aerospace, energy and healthcare industries. The theft of corporate and product data is becoming very widespread, involving in particular software and functionalities that can easily be copied. In Industry 4.0, given that different partners, such as network providers, cooperate between themselves, it becomes easier for these criminals because their attacks can follow many routes and propagate very quickly.

Risks/loss of...	Attacks/threats	Business impacts
Availability	Denial of service DDoS	Productivity loss
		Violation of trade agreements with customers
		Part quality degradation
		Theft of service
Integrity	Critical infrastructure sabotage, machinery or components	Damage to working machinery
		Product quality degradation
		Breach of safety sector standards and regulations
		Violation of trade agreements with customers concerning products
Privacy	Theft of industrial secrets, cyber espionage	Reduction of the business competitive edge
		Damage to the company image and reputation
		Violation of trade agreements with partners concerning data

Table 1.3. *Business impacts related to security threats and filtered by risk (Corallo et al. 2020)*

1.5.3.2. *Denial of service*

DDoS is a cyberattack that aims to make the system unavailable. It can be performed in particular by:

– launching waves of requests on a server to consume all its resources;

– sending malformed input data to crash a process;

– virus infiltration;

– destruction or deactivation of system sensors.

Most devices are interconnected in a factory and, by extension, are interdependent. Consequently, the unavailability of certain devices can be highly critical for a production environment, making these attacks very popular. In addition, with the development of cloud computing, new ways of launching DDoS attacks are emerging, thus driving companies to pay closer attention to them (Haleem et al. 2022).

Unlike cyber espionage in which virtual data is the loss, DDoS attacks have physical impacts with hardware damage such as servers that may need to be replaced (overloading), reconfigured or redesigned.

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

1.5.3.3. *Supply chain and extended systems*

To improve the efficiency of the supply chain, the Industry 4.0 paradigm proposes the connection between several organizational environments. However, the latter exhibits inherent system vulnerabilities that can be exploited by attackers (Ozarpa et al. 2022).

The source of a vulnerability can be a vendor that is the victim of a phishing attack or credential theft, resulting in massive data exposure for the factory.

1.5.3.4. *Smart security and smart factory*

Most manufacturing companies are not fully aware of the security risks associated with the Industry 4.0 paradigm. They usually mainly deal with safety issues when a serious incident occurs.

Nonetheless, technical products by themselves are not enough to manage these risks (Brandao and Duarte 2022). The human factor is an important point. Employee awareness about safety is also important, from skilled machine operators to secure software and planning engineers. This awareness can be achieved in various ways, such as:

– awareness campaigns involving the entire manufacturing environment;

– research groups in higher education institutions that study cybersecurity topics and provide guidelines for industry professionals.

1.5.3.5. *Advanced persistent threats (APT)*

Threats known as APT belong to a specific class of cyberattacks. They are perpetrated by some groups possessing significant experience and resources. The concept is to take advantage of vulnerabilities to infiltrate the victim's network and remain undetected for a long time (Rubio et al. 2019).

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

– network reconnaissance to find vulnerabilities;

– communication to initiate the first intrusion by sending "exploits" to the victim. This can be done directly through social engineering (phishing, etc.), or indirectly by compromising a third party such as the vendor;

– tracking of "zero-day" vulnerabilities to execute remote actions using the "backdoors" of the previous steps;

– propagation to other areas of the network to infiltrate new devices in order to gather information or change the behavior of existing hardware;

– filtering the obtained information to transfer it to the attacker's domain.

The first step is possible due to metadata leaks originating in servers, PLCs and sensors. These issues are inherited from the cloud and IoT paradigms (Rudenko et al. 2022) and need to be solved (Rahman et al. 2022).

1.5.4. *Vulnerabilities, risks and threats by perimeter*

In this section, we analyze security flaws in the various predefined perimeters of the factory. Table 1.4 will be used as a support in the following sections.

1.5.4.1. *Manufacturing-production*

Critical equipment in the manufacturing zone can be reduced to ICSss. From a proprietary and isolated architecture, ICSss have become a standard open platform that is highly interconnected with enterprise and public networks (Asghar et al. 2019). New features, including remote access to networks and terminals, have emerged, enabling a wide range of cyberattacks. In addition, these systems are now available on the Internet.

From 1997 to 2015, the number of vulnerabilities increased from 2 to 189 according to the Kaspersky report in 2015 (Asghar et al. 2019). Most vulnerabilities in production are called "zero-day" because developers have just discovered the existence of the flaw while a patch for fixing it has not yet been released.

The usual reasons behind this are highlighted in Lezzi et al. (2018):

– In factories, devices operate for weeks or months without any security updates or antivirus deployment.

– Multiple intrusion routes (carried laptops, USB drives, etc.).

– No existing isolation between the different networks.

The most common threats in this zone aim at compromising availability and integrity, through in particular physical destruction, DDoS attacks, malware and worms, and "zero-day" attacks.

Physical destruction can fall into the category of typical sabotage of industrial equipment. In the manufacturing sector, DDoS attacks mainly focus on routing with relay attacks, selective forwarding, a gray hole, a black hole or botnets that will affect availability.

Malware and worms will slow down operational performance for the purpose of obtaining sensitive information or modifying device behavior and in the end compromising its integrity. Behavior changes can take many forms, such as tampering with communication protocols by exploiting their weaknesses in terms of authentication and data integrity.

Passive traffic analysis can also be utilized to steal confidential information. The method employed may rely on code injection into operational applications with the aim of corrupting control mechanisms, hacking the end user and then accessing the data.

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

The easy mobility of operators in the factory and their many interactions with mobile devices (laptops, smartphones, tablets) increase the risks associated with these threats.

Applications and device configurations and access controls need to be rigorously verified in this zone.

1.5.4.2. *Logistics*

In the logistics field, many wireless devices exhibit certain vulnerabilities, such as (Kondiloglu et al. 2017):

– Wi-Fi networks, especially when they are not encrypted;

– business applications that still use the HTTP protocol;

– installation of malicious applications.

Network vulnerabilities (unencrypted Wi-Fi, HTTP, etc.) expose almost all information sent by devices to hackers. For mobile terminals, all data scanned with the barcode scanner such as part references, serial numbers, product destinations as well as information about the IT infrastructure such as servers and databases are involved.

The installation of malicious applications could be the source of malware attacks. As an example, “HummingBad” and “HummingWale” affect Android devices and deploy personal data collection applications that are sold in the process.

1.5.4.3. *Active supervision*

The active supervision zone belongs to the company network and mainly includes office equipment. Some possible flaws in this zone are (Kondiloglu et al. 2017; Asghar et al. 2019):

– the lack of antivirus software or out-of-date signatures that could infect the entire industrial control system (ICS) via the Internet and make it unavailable;

– people unaware about security who click on malicious links;

– computers left unlocked when leaving the office;

– access to unauthorized files/websites/data;

– connection to external devices;

– installation of unlicensed (pirated) programs.

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

– social engineering attacks (phishing);

– network attacks;

– viruses, malware, worms and ransomware;

– theft, loss or hardware and data failure;

– data transfer to and from unauthorized devices.

1.5.4.4. *Research and development*

This zone contains innovative equipment that can become a source of potential threats due to a lack of perspective on the technologies used. This zone can also be targeted by attacks because of the confidential and valuable information that attackers might find.

1.5.4.5. *Living zone*

In the living zone, VoIP phones are the main equipment identified. While VoIP allows businesses to save on network costs, it also brings about new threats and security risks (Omari et al. 2022). Some of these risks are common, such as DDoS attacks that overwhelm the VoIP server with SIP (Session Initiation Protocol) call signaling messages. Such attacks are dangerous because they do not require penetration of the entire network.

Viruses and malware can also affect VoIP phones because VoIP configurations make use of "softphones". With VoIP networks, mobile malware is also a problem as many users make VoIP calls with their smartphones. This means that once the malware has infiltrated the smartphone, it can access and steal valuable information.

Another threat is *vishing*, which is the vocal counterpart of email phishing. Employees, suppliers and customers are required to share sensitive information.

Phreaking occurs when a hacker gains access to a company VoIP network and uses it to steal corporate data, change the network plan, or make expensive calls, resulting in huge costs for service providers.

Eavesdropping is also a common cybersecurity threat that is very difficult to prevent. Hackers are able to access and listen to VoIP calls by capturing unencrypted VoIP traffic. In this way, they are capable of performing identity theft, as well as theft of VoIP services.

The latest threat is *Spam Over Internet Technology* (SPIT). For hackers, this consists of capturing thousands of VoIP IP addresses and then sending voice messages to a VoIP system.

1.5.4.6. *External zones*

Outdoor spaces are divided into two categories which are physical and virtual.

1.5.4.6.1. Physical external zone

The physical external zone consists of IP surveillance cameras that fall under the umbrella of the IoT. Threats to these types of devices include:

– interference with the routing protocol mode of operation by way of jamming and interference in order to disrupt communications;

– resource exhaustion through the use of vulnerabilities in software that controls devices or with malicious code (*malware*);

– manipulation of routing information to influence traffic, as in a Sybil attack (Rubio et al. 2019). These attacks are gateways to others, such as black hole or denial of service;

– side-channel attacks to expose device information (battery, memory) or routing and topology information to identify vulnerable devices in the infrastructure;

– injection of fake nodes that can execute code or inject illegitimate traffic in order to control large areas of the network or to eavesdrop;

– poor access control resulting in unauthorized access to protected resources.

1.5.4.6.2. Virtual external zone

The second category is the virtual external space, which encompasses everything related to cloud computing. The latter is attractive due to its low investment cost and how easily companies can deploy it. Many organizations resort to cloud computing for storing their data, but also for hosting certain processes. It can even be used on the IoT to acquire sensor data, but also as a way for customers to manufacture a product through a shared network of suppliers throughout its lifecycle. These innovations introduce the following threats:

– DDoS attacks that exploit vulnerabilities inside the scheduler component of some hypervisors to charge for the service and make it unavailable (Rubio et al. 2019);

– malware injection to replace a legitimate cloud instance service such as a virtual machine with a malicious service to access the exchanged data;

– side-channel attacks that force machines to study electromagnetic radiations and access their resources;

– shared memory attacks that analyze the cache or main memory to obtain technical information about the infrastructure, running processes or to access the memory dump of virtual machines;

– social engineering attacks that capture customer information from different applications. The objective is to obtain sensitive data such as accounts and passwords in order to host malicious services in the cloud.

Most of these attacks are referred to as advanced persistent threats (APT), which can be executed primarily by experienced, resourceful attackers. It should be noted that here we have not considered data sovereignty-related risks and geopolitical risks, when cloud services do not fall under the legislation of the country in which the factory is located.

1.6. Review of cybersecurity solutions

This section will provide a detailed examination of some of the existing solutions against cybersecurity threats. These solutions have been selected in order to present the main trends concerning conventional and innovative solutions that can be applied in the different perimeters defined above.

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

1.6.1. *Definitions*

1.6.1.1. *Countermeasures*

Countermeasures can be seen as the short-term defense mechanism against a threat or attack. They represent a set of actions and techniques to eliminate a threat or prevent it in order to limit the damage it could cause. They can also help flag the threat so that corrective action can be taken (Lezzi et al. 2018).

1.6.1.2. *Solutions*

Solutions are the long-term way to deal with threats. They are often defined with different names such as approach, methodology or architecture. They represent a comprehensive set of actions for protection against different types of cyberattacks. These solutions can be classified into three categories (Asghar et al. 2019): security assessment tools, intrusion detection and prevention technologies as well as ICSs risk management.

	Possible threats in perimeters					
	Threats	**Manufacturing-production**	**Logistics**	**Active supervision**	**Living areas**	**External areas**
Availability	Device hijacking	X				
	DDoS attacks	X	X	X	X	X
	Path attacks	X	X	X		
	Node resource depletion	X	X	X		
	Service theft	X	X			X
Integrity	Incorrect configuration	X	X			X
	Malware injection	X	X	X	X	X
	Fake data injection	X	X			
	Identity theft	X		X	X	
	Routing information tampering	X	X			
Confidentiality	Sensitive data theft	X		X		X
	Node state exposure	X	X	X	X	X
	Passive traffic analysis	X	X	X	X	X
	Infrastructure-related information exposure	X				X
Authentication	Privilege elevation	X		X		X
	Social engineering	X		X	X	X
	Inefficient access control	X	X	X		X
	Node identity theft	X	X			

Table 1.4. *Risks and threats by perimeter in Industry 4.0*

Security assessment tools are able to provide secure experimentation with realistic test scenarios (attacks, infections, etc.) in order to detect security issues before initiating production.

Intrusion detection and prevention technologies highlight approaches to securing ICSss by introducing new components or upgrading existing architectures. For the management of ICSs risks, guidelines, standards and measures are proposed to ensure that the security implemented is protected against developing threats.

1.6.2. *Cybersecurity countermeasures*

According to Lezzi et al. (2018), the following three-tiered approach can be used to ensure the security of ICSs:

– perimeter hardening by isolating the factory network from the office network using firewalls and a demilitarized zone (DMZ);

– network multi-layered defense to contain attacks;

– user isolation within a separate zone/network.

Countermeasures	Protects against/prevents
Communication encryption	Data corruption Information disclosure
Stored data encryption (signature)	Repudiation attacks
Data stream encryption	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 (system, software, business, firmware)
Secure communications (VPN, Wi-Fi and IP)	Eavesdropping Unauthorized connection Data analysis
Antivirus and anti-malware	Malware

Table 1.5. *Countermeasures for cybersecurity in Industry 4.0 (Lezzi et al. 2018)*

These measures enable protection against unwanted access to and from the Internet, but are also used for keeping services and zones separated between plant systems. Encryption is the most popular of these measures and is available at several levels:

– communication encryption to prevent information tampering and disclosure;

– encryption of stored data to prevent repudiation attacks;

– data stream encryption to avoid all previous problems.

To be effective, all countermeasures must be continuously updated, including encryption protocols, firewall signatures, security controls (patches), and monitoring (log analysis). Table 1.5 describes the most popular countermeasures summarized from Lezzi et al. (2018) and how they can help prevent cyber threats.

1.6.3. *Proposals for cybersecurity solutions in the literature*

This section will highlight and present in detail some of the cybersecurity solutions currently available in the literature (Table 1.6). For each solution, we describe its purpose and design structure, as well as an evaluation of how it has contributed to improving cybersecurity.

1.6.3.1. *Protection of physical environments*

1.6.3.1.1. Background and goal

Modern businesses need both software and physical solutions for the security of their information. Despite the effectiveness of software controls, these remain virtual and there is always the possibility that an interface may escape the control of the system and compromise it. This interface can be human, and the flaw appears when information is verbally exchanged. In addition, the explosive growth of wireless networks in information system architectures has further increased the possibility of information leakage (Illési et al. 2018). For these reasons, Kiss et al. (2019) proposed the creation of a physical information security mechanism. This solution is implemented in the form of "protected zones" (Figure 1.5), which designate spaces where sensitive and valuable data can be securely exchanged, both acoustically and visually.

1.6.3.1.2. Design and approach

This solution aims at the following goals:

– prevent access to unauthorized persons;

– restrict information propagation to the limits of protected zones;

– maintain a homogeneously protected and controlled environment.

To achieve these objectives, three layers of solutions are proposed.

The first layer consists of the conventional mechanisms used to defend protected installations: admission authentication, people screening, definition of authorizations and security systems.

With the first layer, we can be sure that the people present in the zone are all authorized, however there is always a risk because the information can still be "eavesdropped" by someone outside.

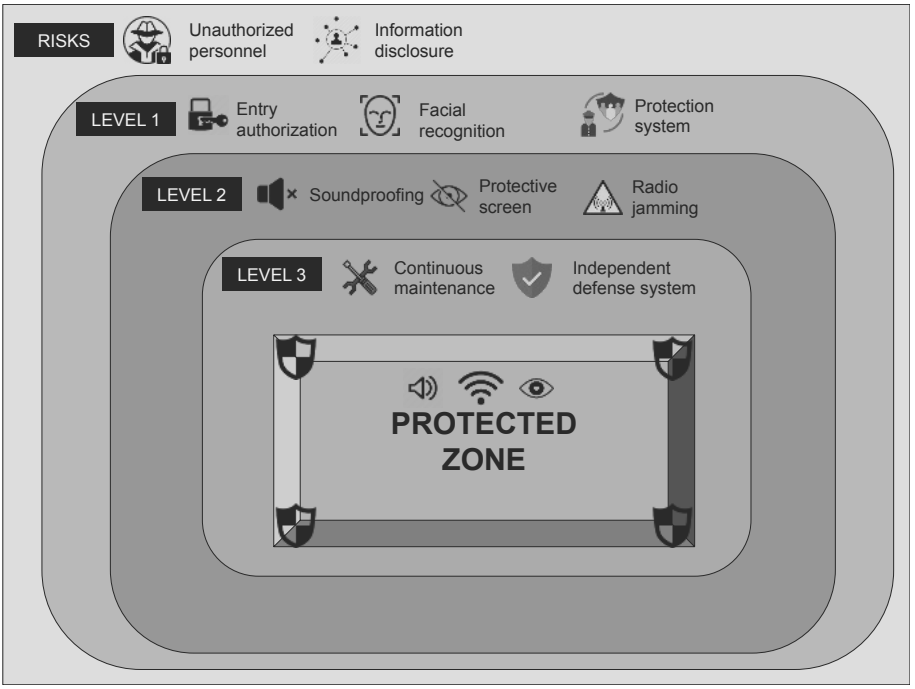

Figure 1.5. *Protection of physical zones*

The second layer takes care of the prevention of information transmission outside the protected zone by physical characteristics (visual, sound, radio) through the use of acoustic shielding, visual shielding and radio shielding.

This security proposal defines the last layer as being responsible for maintenance, which involves continuous maintenance and an independent defense system.

The idea underlying maintenance is to preserve the homogeneity of the environment, search for alien objects and monitor radio signals. An autonomous safeguarding and surveillance system has also been recommended to complete the security of these protected zones.

1.6.3.1.3. Results and highlights

The author suggested that although new technologies introduce new threats, the preparation and creation of these controlled zones jointly with other actions could result in preserving integrity, confidentiality and availability in the long term.

1.6.3.2. *Firewall for Industry 4.0*

1.6.3.2.1. Background and goal

The manufacturing execution system (MES) is the intermediate system between the ICSs and enterprise applications such as enterprise resource planning (ERP) software. It improves the transparency of manufacturing data. Sensor data can be used to compute real-time performance indicators or monitor machine status and the quality of manufacturing processes. Improved interconnectivity of IT systems exposes devices such as PLCs to cyberattacks, which could disrupt production or infect other systems. The most widespread attacks concerning the MES are based on network scanning/probing where defense-in-depth is an efficient countermeasure. Cybersecurity standards typically proposed network architectures split into several segments including firewalls in between them to minimize security risks. Given the need for defining configuration rules in a flexible and secure way, software-defined networking (SDN) is probably a key technology for this purpose (Nunes et al. 2014; Satasiya and Raviya Rupal 2016). Another recent related proposal focused on network performance is presented in Zeng et al. (2019). Software-defined networking (SDN) is a technology capable of network alternation, releasing critical information and providing new services to run on-demand applications. It provides a clear overview of the network architecture to administrators and allows users to programmatically control the network architecture. This means that it is possible to modify network access on demand and minimize the exposure of ICSs networks to attackers. On this topic, Tsuchiya et al. (2018) proposed a protection network structure based on an SDN firewall specifically designed for industrial networks, without jeopardizing network flexibility (Figure 1.6).

1.6.3.2.2. Design and approach

The proposed solution has three objectives:

1) the creation of segments without reconfiguring existing networks, while using a DMZ (demilitarized zone) vertical integration;

2) the development of one-way access mechanisms (server access only when a client requires a connection);

3) the reduction of flaws in access rules due to the frequent addition or replacement of devices in certain zones.

The two main functions of the SDN firewall are packet filtering based on automatically applying access rules to a group of devices as well as operating as a gateway between network interfaces to avoid any changes to the existing network configuration.

This packet filtering function means that only whitelisted applications are authorized to access industrial control devices. The whitelist is managed by network administrators, whose management task is greatly simplified, because it is the only

thing that needs to be done to comply with the security standards of ICSss. At the component level, the firewall contains:

– the transparent firewall that applies access rules and implements an access control system based on the OPC UA standard;

– the firewall controller that stores the production system configuration and manages the rules.

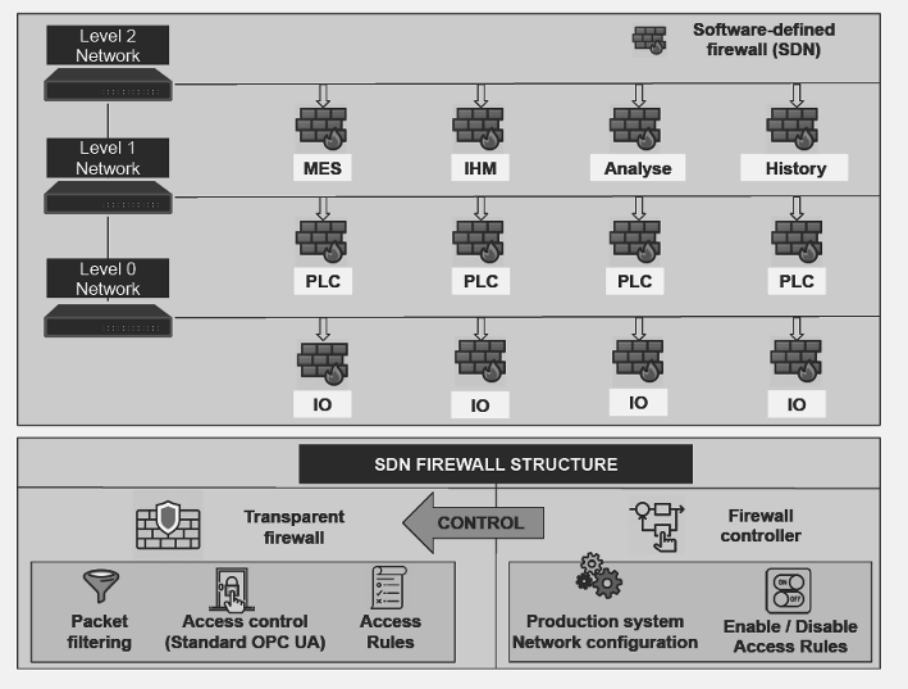

Figure 1.6. *Software-defined firewall (SDN)*

The Open Platform Communication Unified Architecture (OPC UA) standard used for access control in the transparent firewall is a machine-to-machine communication protocol for industrial automation.

This is an improved development of the original OPC protocol to satisfy the emerging requirements of industrial automation in Industry 4.0. Its most significant innovations are:

– cross-platform implementation;

– scalability (smart sensors, smart actuators, etc.);

– multi-thread or single-thread;

– security enhancement (new standards);

– configurable waiting times;

– chunking of large datagrams.

Security in OPC UA consists of authentication, authorization, encryption and data integrity relying on signatures. In addition, the communication stack makes use of firewall-compatible transmissions, which is why this standard was used to design the SDN firewall.

1.6.3.2.3. Results and highlights

The author confirmed that the solution was tested in the virtual network of a full environment (OPC client/server with machine data exchange) and that the firewall was able to prevent the security scanners from taking control of the application port and other details at the OPC server operating system level.

The implementation of the prototype allowed us to improve the security features of the OPC UA standard and provided a comprehensive security solution for ICSs networks.

1.6.3.3. *Security in IoT devices*

1.6.3.3.1. Background and goal

The IoT is a term that was first employed by Kevin Ashton in 1999 (Ashton 2009). There is no universal definition of the term, however it suggests that any everyday object can be equipped with the capability to measure anything related to its environment, communicate with other objects and send the detected data through the Internet (Whitmore et al. 2014). In a factory, it connects several technologies related to sensor development and machine control. In the context of Industry 4.0, they are becoming popular due to the interconnection between data from industrial workshops and the possibility of providing feedback about system operation. Their use leads to the new concept of CPSs, which are associated with the implementation of the IoT, and involve the use of sensors for collecting, processing and utilizing data in the cybernetic world. In terms of IoT hardware connectivity, there are emerging networks called Low Power Wide Area Network (LPWAN), such as Sigfox, LoRa and Weightless (Ali et al. 2017). These networks are specifically designed for the IoT because they are low power consumption protocols. Furthermore, they enable two-way communication between objects and the outside world using the LPWAN network and the network provider's cloud for internet connectivity.

The main underlying drawback that hampers a wider acceptance is their weaknesses in terms of cybersecurity (Atzori et al. 2016), which are caused in particular by the heterogeneous connectivity and the threats deriving thereof (breach of privacy, etc.), and can lead to serious consequences for IoT technology users (Lin

et al. 2017). According to Wolf and Serpanos (2018), these systems must be designed and operated following a unified view of safety and security features (Miraz et al. 2015). In the context of the smart factory, one of these threats could be the result of weaknesses linked to the use of cloud computing (Hassija et al. 2019). With these considerations in mind, an ontology-based cybersecurity framework for the IoT was proposed by Mozzaquatro et al. (2018).

1.6.3.3.2. Design and approach

The proposed framework focuses on:

– business-side monitoring;

– security analysis and classification in a knowledge base;

– the design of security services;

– improved security mechanisms for business processes and technology assets.

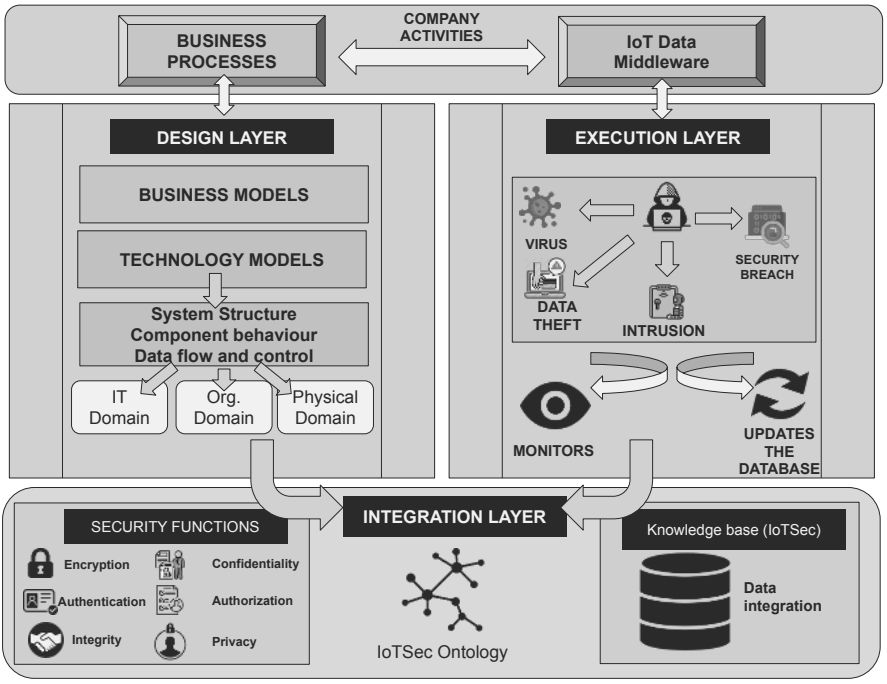

Figure 1.7. *Ontology-based framework for IoT cybersecurity*

Figure 1.7 is a representation of the framework architecture. It is broken down into three layers: two layers that deal with cybersecurity at design and run time, and the integration layer used during both stages. The concept behind the design layer is as

follows: it is assumed that a company needs to implement specific services at all times in addition to those already in use, which requires adaption in order to meet the device constraints.

The Model-Driven Service Engineering Architecture (MDSEA) is a software development methodology that focuses on creating and making use of conceptual models (for the framework: business models, technology-independent models and specific models) related to a specific problem. Using this methodology, the design layer is capable of generating code from a high level of abstraction to accelerate service design and adaptation, as well as deployment time. Managers can then collaborate with developers and contribute to building new features.

The runtime layer has two goals: to monitor and update the knowledge base. Monitoring is the process of detecting intrusions, data theft, viruses and any other attempt to exploit security vulnerabilities. All these situations are analyzed to identify the appropriate solutions among the IoTSec pool of security services in order to restore the system and improve cybersecurity. Updating consists of adding detected threats and security analysis to the knowledge base, preventing these threats from reoccurring. The data integration layer provides information on threats and vulnerabilities based on the IoTSec ontology, which is an ongoing work of Mozzaquatro et al. (2015).

1.6.3.3.3. Results and highlights

Finally, the authors consider that the cybersecurity ontology improves the efficiency of security operations and helps analysts extract relevant information to characterize vulnerabilities. However, a number of questions remain open before obtaining a multi-layered cybersecurity intelligence ontology capable of understanding potential threats in the context of cybersecurity, which is a constantly developing area.

1.6.3.4. *Authentication of cyber-physical systems*

1.6.3.4.1. Background and goal

Long value chains are one of the main security issues of Industry 4.0. Information Technology (IT) paradigms do not reflect the particular circumstances found in operational technology (OT).

Data of many kinds are accumulated in the production zone, and are used for quality control and predictive maintenance. However, only some of them are critical to protection. An OT solution should focus on nomenclature, design information and control parameters (Wegner et al. 2017).

In the manufacturing environment, the architecture currently in use is in general entirely separate from production environments, with isolated manufacturing devices.

There is no control over contractors in multi-stage production when data are no longer on the server.

Similarly, operators are not supervised once the data are received and many issues arise, such as data corruption. As established by Pan et al. (2017), the threats identified for additive manufacturing apply to digital manufacturing devices of all shapes and sizes. Consequently, a new paradigm is proposed by Wegner et al. (2017). It aims to limit and protect the flow of information in devices used during the outsourced stages to enhance perimeter security.

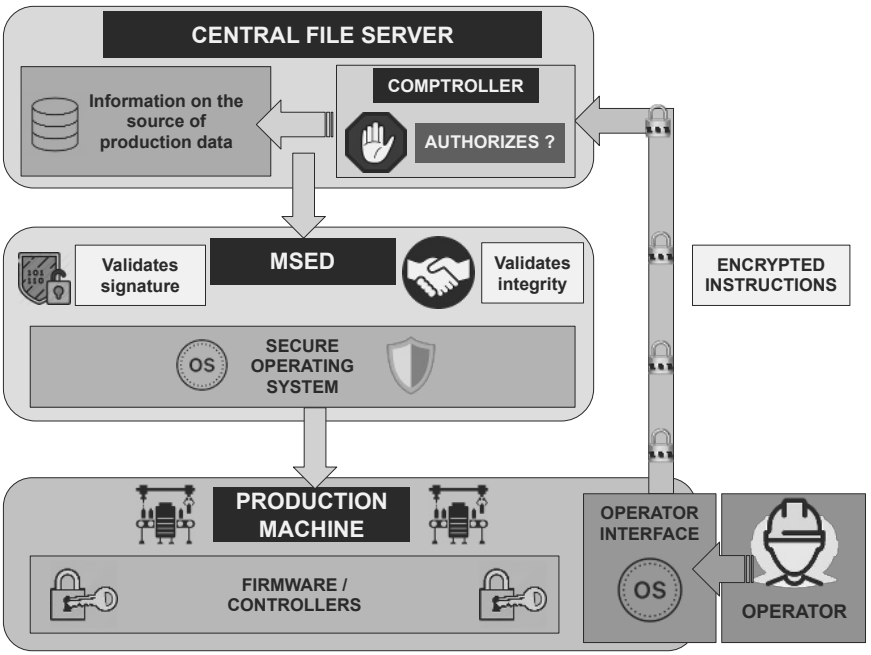

Figure 1.8. *Direct-to-machine approach for the protection of manufacturing cyber-physical systems*

1.6.3.4.2. Design and approach

This new manufacturing information architecture is based on the holistic approach according to which data must be sent directly to the relevant manufacturing device. This approach is also called direct-to-machine communication (Figure 1.8). The fundamental security issue underlying it concerns authentication and authorization:

– Is the request sent to the device authentic?

– Is the sender allowed to send this request?

To solve this problem, the proposed architecture comprises two components. The first one is encryption with a manufacturing security enforcement device (MSED). It relies on asymmetric cryptography. The public key is used to verify that actors or entities have the proper private key, thereby authenticating them.

The second is a software program called "comptroller" that runs on a production network and authorizes every action taken. It takes the input data, provides a key and stores the output data. Output data are appended at the end of a virtual document, which is the provenance record of a produced part. The data transmitted between the "comptroller" and the production device will then be processed by a MSED whose exhaustive description can be found in Graham et al. (2016). The MSED is located upstream of the manufacturing equipment and authenticates manufacturing instructions issuing from the cloud by verifying both the integrity of the instruction data, as well as the "comptroller" identity and permissions. To this end, the best method consists of using encryption and unique data signatures to ensure that the data source is authentic. Another requirement for the MSED is to have a secure operating system (OS). Common operating systems for embedded systems are Microsoft Windows™ or Linux™. They provide a wide range of tools, but are vulnerable to zero-day attacks that can prove devastatingly effective. Wegner et al. (2017) mentioned smaller operating systems such as SeL4, whose security have been formally verified.

1.6.3.4.3. Results and highlights

An MSED device prototype using the SeL4 microkernel has been developed in collaboration with True Secure SCADA, LLC and has been confirmed to be compatible for general industrial control as well as manufacturing.

There are strong arguments supporting direct-to-machine communication for overcoming cyber-physical security challenges, namely:

– its characteristics (operator authorization, monitoring and control, device support, distributed responsibility, location independent);

– its contrast with existing solutions (built-in security, layered-based encryption, always up-to-date, integrity protection, minimized sharing);

– its role of building a responsive production environment (detailed monitoring with the controller, collaboration, distributed manufacturing, automation).

One of the challenges concerning the adoption of this approach is the willingness to manage a higher security level at the cyber-physical scale, or that IT services acknowledge production hardware as another digital component to be included in the list of elements to be protected. In Industry 4.0, these devices are no longer separated from the data flow, and the direct-to-machine approach acknowledges this fact.

1.6.3.5. *Predictive cyberattack detection*

1.6.3.5.1. Background and goal

Conventional cybersecurity architectures focus on mechanisms that guarantee confidentiality, authentication, integrity, access control and non-repudiation to prevent network intrusions and attacks. Nonetheless, the existing security landscape is characterized by large, fast, persistent and highly sophisticated continuously changing attacks.

For critical systems belonging to Industry 4.0, autonomous detection and response to cyberattacks is required in order to achieve robust cybersecurity with defense-in-depth. A cyberattack detection algorithm has been proposed by Thames and Schaefer (2017) to defend Industry 4.0 systems, as well as other internet-based systems. This algorithm is based on ensemble intelligence with neural networks to utilize a classification output providing feedback to active response mechanisms. The underlying goal is to show how computational intelligence-based approaches can be employed in Industry 4.0 cybersecurity.

1.6.3.5.2. Design and approach

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

Computational intelligence systems (CISs) are adaptive systems endowed with decision-making capabilities, and they are specifically designed to manage large volumes of data (with noise) in their decision-making process. Therefore, they appear to be a logical choice when designing new algorithms for detection systems. These systems use technologies such as *Machine Learning* and *Deep Learning* that are able to accurately discover the essential differences between normal and abnormal data (Zhao et al. 2017; Liu and Lang 2019).

The proposed classification algorithm is called Neural Network Oracle (NNO) and includes three components: neural networks, genetic algorithm and the NNO.

Figure 1.9 is a representation of the ensemble intelligence framework that uses the NNO classification algorithm for predictive cyberattack detection in advanced manufacturing.

Neural networks, also known as artificial neural networks (ANNs), loosely mimic biological processes and are used to solve AI problems. One of their most interesting characteristics is training-based self-learning with datasets. In the NNO, a collection of neural networks will train with a first set of audit data. The result of this first classification will then be sent to the NNO.

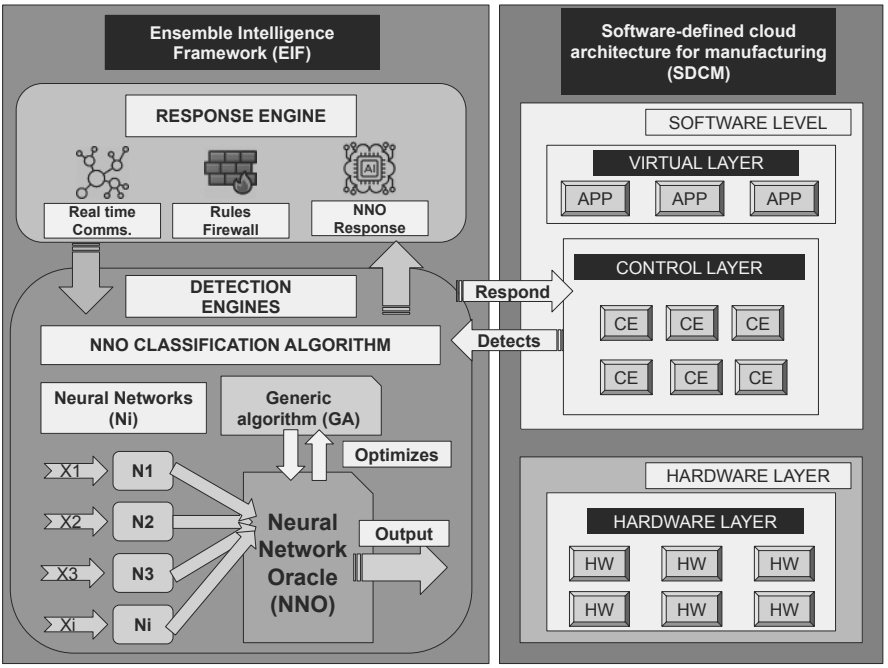

Figure 1.9. *Predictive cyberattack detection with ensemble intelligence in advanced manufacturing*

The genetic algorithm (GA) is based on the process of biological evolution and the ability to adapt over time to 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 accuracy. To obtain these optimal parameters, a fitness function evaluated with the neural network responses is used.

The neural network oracle is trained with a secondary dataset consisting of the outputs from the previous neural networks and the original dataset. To minimize errors, it utilizes the optimal parameters provided by the genetic algorithm.

1.6.3.5.3. Results and highlights

The author integrated the NNO classification-based ensemble intelligence framework into a software-defined cloud architecture for manufacturing (SDCM) (Thames and Schaefer 2017). The SDCM is divided into three layers: virtual, control and distributed hardware.

Given that the control layer is the one with the best knowledge of activities and communications, it will be employed as a data collection point. The control layer will

continuously feed the ensemble intelligence framework (EIF) with data, and the EIF will be responsible for analyzing the detected data and solving the detected anomalies.

In terms of performance, the NNO was trained and tested with the *CUP99* intrusion detection dataset, and achieved a good classification performance. It was concluded that it could be coupled with active response mechanisms within the framework of Industry 4.0 to counter cyberattacks.

1.6.3.6. *Predictive maintenance system protection*

1.6.3.6.1. Background and goal

ICSs have been increasingly targeted by hackers since the beginning of the 21st century due to the potentially significant damage they could inflict on the system and its environment if the attacks are successfully executed. The ICS network can be broken down into three levels (McLaughlin et al. 2016; Sicard et al. 2018):

– level 0: the operational part with sensors/actuators;

– level 1: the control part with PLCs/HMIs;

– level 2: supervision with control room/SCADA.

IT solutions such as firewall/DMZ are typically used at level 2 and above for protection against DDoS or Man in the Middle (MITM) attacks. Solutions in this layer work well because they are very similar to traditional IT infrastructure.

However, these solutions do not work in real-time layers 0 and 1, which have their own inherent attacks (random attacks, fake data injection). Four types of attacks are considered: namely direct, sequential, time-based and over-solicited attacks.

An innovative methodology was proposed by Sicard et al. (2019) based on the concept of "automation knowledge". This is an in-depth study of Sicard et al. (2018) by the same author. The solution will focus on the protection of low-level elements (level 0-1) such as PLCs, computer-integrated manufacturing (CIM) architecture sensors, taking into account safety and security aspects. The final objective is to be able to detect malicious commands issued by the PLC.

This approach can be seen as a last shield to protect the system from cyberattacks assuming that hackers have already broken through the previous defense levels.

1.6.3.6.2. Design and approach: models and filters

The first step is based on behavioral patterns (Mitchell and Chen 2013), which represent the normal operation of the system. It is divided into four parts:

– risk assessment to determine the critical zones to be protected (prerequisites);

– parameter identification (offline);

– control of the filter model generation (offline);

– execution of detection mechanisms during operation (online).

Risk assessment is a prerequisite. The methodology assumes that a risk analysis has been performed with the system. This analysis should highlight the events that could be harmful to the system and infer which part of the ICSs should be protected first. To this end, the input/output (I/O) list of the PLC has to be modeled.

Parameter identification consists of creating the states from the I/O list created by the risk assessment. This will help define both the scope and the states used in the behavioral models. Mathematically, these states are defined with combinatorial constraints based on the values of the sensors and actuators. The following types of states are accounted for in an ICS:

– optimal (compliance with the control law as well as the physical constraints of the system);

– dangerous (compliance with the physical constraints of the system only);

– forbidden (damage to the physical system);

– accessible (all admissible states);

– inaccessible (all states to avoid).

Next, time constraints must be determined to identify time-based attacks. These time specifications introduce another dimension to the characterization of the system behavior as well as another protection level for the ICSs. The use of combinatorial and time constraints is required to ensure the efficiency of detection algorithms.

The generation of the control filter model is intended to represent the industrial system with the process and control model. The operation stage corresponds to the availability of the control and report filters in the ICSs. These filters should be located just after the sensors to ensure command integrity and to detect any malicious behavior (Figure 1.10).

The next question consists of determining the desired protection level with these filters. Three levels of security are taken into account:

– goods and people security: guarantee a set of states according to which the system can develop without danger;

– quality: guarantee the proper execution of the control law and monitor the system;

– equipment protection: monitor actuator loads under overly intense or too frequent commands (in order to reduce wear, risk of failure and equipment maintenance).

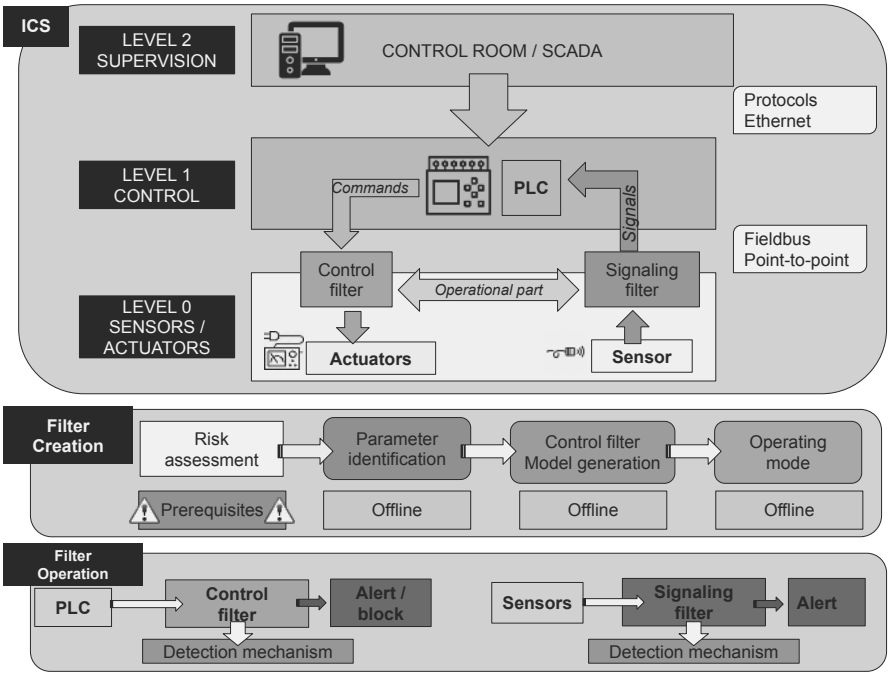

Figure 1.10. *Filter implementation in the behavioral model approach for the protection of industrial systems*

1.6.3.6.3. Design and approach: detection based on the notion of distance and trajectory

The filters described in the previous section allow the implementation of rules, but they can only block attacks when the critical state is about to be reached. A mechanism for detecting deviations from normal behavior is necessary to implement an exhaustive methodology. This mechanism is based on three notions, which are distance, the shortest path to the critical state and trajectory. Figure 1.11 is a simplified representation of the proposed detection mechanisms.

The notion of "distance" is linked to the ICSs states and was introduced in Carcano et al. (2011). It represents the deviation between the current state and a set of critical states, all of which are states that the system should not reach. The benefit of this concept resides in the fact that it provides operators with indications about proximity to the critical zone. The "shortest path to critical state" is the smallest number of commands that must be applied before reaching a critical state. The overall goal is to calculate, for each achievable state, the closest distance to a critical state. These computations are performed offline and integrated into the filters to

perform the detection algorithm, while taking into account real-time constraints. The last notion is that of "trajectory", which is complementary to the notion of distance. The distance only provides specific information about the system, but trajectory is defined as "the evolution of distance according to the state or time sequence".

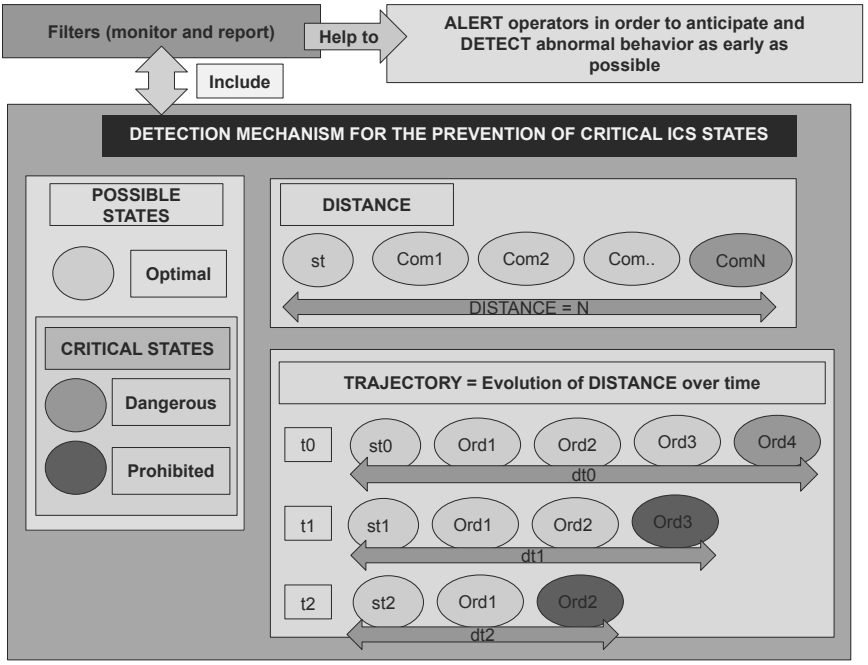

Figure 1.11. *Distance and trajectory-based critical state detection mechanism for the protection of industrial systems*

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

– context detection;

– anomaly detection (combinatorial and temporal);

– equipment degradation.

The main advantage of the proposed mechanisms is that operators receive warnings, deviations are anticipated and abnormal behavior detected at its earliest stage.

1.6.3.6.4. Results and highlights

The author confirmed that the approach showed good results for detecting cyberattacks that affect physical systems. The particular improvement could be seen in blocking commands before driving the system into a critical state, and in detecting sequential attacks using combinatorial and time constraints. However, some improvements were proposed, such as:

– using a safety/security approach to improve the effectiveness and consequently the number of attacks accounted for;

– considering the system behavior between two stable states.

1.6.4. Honeypots *and* digital twins

1.6.4.1. *Overview*

Several innovative solutions can be found in the literature, namely the cybersecurity immune system for Industry 4.0 (Petrenko 2020), to name just one. However, in this book, we will focus on two popular approaches: *honeypots* and *digital twins*. Honeypot systems are passive monitoring systems capable of early alerts in production environments and critical infrastructure. Their main feature is to issue alerts if the infrastructure has been penetrated by hackers or malware-related activities.

Technically, a *honeypot* consists of data that appears to be a legitimate system component presenting valuable resources for attackers. However, in fact, the *honeypot* is isolated and monitored to block or analyze attackers. In more specific terms, the idea is to bait attackers. The main advantages of this solution are:

– awareness that someone or something is trying to exploit your company's critical systems;

– the attacker loses valuable time attacking a decoy system, instead of the real infrastructure;

– more time is thus given to the security team to block the attack;

– the company will not waste time with false positive alerts because there is no reason for any communication to take place from or to the *honeypot* system.

1.6.4.2. *Honeypot-based solutions*

Existing honeypot-based solutions are usually distributed systems capable of collecting and analyzing threat or attack-related information (Rubio et al. 2019). The purpose of this analysis is to determine the type of attack, the existence of infected devices, as well as the activities carried out with the system.

Cybersecurity solutions	Concerned equipment	Protects from...	Concerned factory perimeter(s)
Physical environment protection	All	Unauthorized physical access, information spreading (acoustic, visual, radio)	All
Software-defined firewall	Manufacturing Execution System (MES)	Network scanning	Manufacturing-production
IoT ontology framework	IoT devices	External attacks (viruses, data theft, security breaches)	Manufacturing-production/logistics
Cyber-physical system direct authentication	Cyber-physical systems (CPSs)	Unauthorized instructions to production machinery	Manufacturing-production
Advanced manufacturing set learning framework	Industrial control systems (ICSs)	Predictive cyberattack detection using neural networks	Manufacturing-production
ICSs predictive maintenance by establishing behavioral models	Industrial control systems (ICSs)	Predictive cyberattack detection using the notion of distance and critical states (sabotage detection, for instance)	Manufacturing-production

Table 1.6. *State of the art of cybersecurity solutions in Industry 4.0*

1.6.4.2.1. Attica Networks ThreatMatrix

ThreatMatrix is Attica Networks' leading honeypot-based detection platform capable of detecting intrusions in real-time in ICSs/SCADA systems as well as IoT environments (Rubio et al. 2019). Its flagship product, BOTsink, is able to detect APTs without being detected by attackers. Other features also include software images to simulate SCADA devices as well as their protocols, so that they cannot be distinguished from real devices.

1.6.4.2.2. Industrial Defenica ICS Honeypot

In 2018, a worldwide study conducted by the Ponemon Institute on behalf of IBM found that the average time needed to identify a data breach is 197 days. Moreover, the most well-known attacks in industrial environments involved hackers who had penetrated inside the network for at least 3 months before being detected. Based on these results, Industrial Defenica proposed a high-interaction honeypot for ICS/SCADA industrial systems.

This solution employs advanced deception technology capable of presenting fake model-based units (PLC, Ethernet-serial devices) in the network. More than 3,500 different devices can be tampered with (protocols, services, open ports, etc.), and these tampered devices can communicate with real ICS devices. Many steps are necessary for attackers to determine if they are dealing with a real device, and these steps would alert the security team that someone is breaking into the infrastructure.

To provide the best possible data about threats, a worldwide ICS Industrial Honeypot network was created to gather feedback from deployed solutions, as well as to improve data, equipment support, better equipment profiles so that they continue to appear as credible simulators.

1.6.4.3. Digital twins *for cyber-physical systems*

Digital twins were recognized as one of the top strategic technology trends of 2019 by Gartner (Eckhart and Ekelhart 2019). Here, we focus on a few use cases that demonstrate how they can harden the security of cyber-physical systems.

1.6.4.3.1. Definition

The standard definition of digital twins is that they are virtual replicas of physical objects that serve to monitor, visualize and predict the states of cyber-physical systems. Within the context of information security, Eckhart and Ekelhart (2019) has proposed a uniform definition based on the literature: a digital twin is "a virtual replica of a system that follows its physical counterpart during all the stages of its lifecycle, consumes real-time and history if necessary, and is realistic enough to allow the implementation of the desired security measure". Another term is also mentioned concerning digital twins: digital thread. In Eckhart and Ekelhart (2019), digital thread is defined as "the uninterrupted data link throughout a system lifecycle that can be used to generate and deliver updates to a digital twin".

1.6.4.3.2. Use cases in the manufacturing sector

Several use cases have been identified with digital twins operating to secure manufacturing systems:

– CPSs secure design;

– intrusion detection;

– misconfiguration detection (hardware and software);

– security tests;

– intimacy;

– system testing and training;

– secure dismantling;

– security and legal compliance.

To design more secure CPSs, digital twins should be used in combination with a virtual environment to analyze system behavior under attack. This would thus allow engineers to estimate potential damage, thereby facilitating the process of designing safety and security mechanisms to produce in the end more robust and fault-tolerant CPS architectures. Digital twins could also help identify weak points in the architecture or unnecessary features in devices that could contribute to exposing them to intrusion.

Digital twins can also help set up intrusion detection systems (IDSss). In this regard, Eckhart and Ekelhart (2019) presented a passive state replication approach that aimed at replicating a state from a physical device to a digital twin. This allows the digital twin to reflect the behavior of the actual CPS during its operation. Next, it is necessary to implement a behavior specification-based IDSs in which the normal CPS behavior is correctly defined to detect any changes. This technique presents low rates of false negatives and can detect certain attacks that were not known at the time the legitimate behavior was defined. Finally, intrusions can be simply detected by comparing the inputs and outputs of physical devices and their associated digital twins.

Since digital twins are the result of hardware and software emulation of devices, they mimic similar functionality. A hardware and software misconfiguration will be detected when different behaviors are observed between digital twins and their physical counterpart. If a difference is observed, it could indicate malicious actions. Unlike traditional configuration data analysis where only the software is verified, this use case also applies to hardware.

Security testing in operational environments (OT) is essential because it is performed on live systems and can cause serious damage or business interruption. Test benches are normally used to avoid interference, but their maintenance is costly in terms of time and effort. Digital twins enable security tests to be performed virtually instead of conducting them on real systems. How realistic a digital twin appears is a critical point, and this use case could also apply early in the engineering phase to fix vulnerabilities in the cyber-physical system. Using a digital twin as a honeypot system during the operational stages could also make it possible to test the security of the CPSs with real attackers and help harden the actual security of CPSss.

The concept of digital twins can also facilitate privacy protection, for example, by helping controllers or processors comply with the requirements of the General Data Protection Regulation (GDPR) (for instance, an insurer offering an insurance product based on data obtained from smart car digital twins). As digital twins use certain methods to classify data that can be anonymized before the data are transferred to the owner, privacy rights can be preserved.

Because digital twins are virtual and operate in an isolated environment, they can be used as a testing and training platform. The purpose of this platform could be to

test new defenses or to train to control cyberattacks. The main idea is to launch attacks against digital twins from the virtual environment for testing and training purposes.

When the ICS and CPS reach end of life, the components must be disposed of in a secure manner. Several aspects have to be considered, such as data privacy requirements, as well as costs associated with disinfection. Digital twins could facilitate the secure disposal of physical devices. However, they can be affected by unauthorized access. It is therefore important to make sure that the digital thread is severed and correctly archived.

It seems that regulatory requirements for CPSs operators are increasing, which is the reason why digital twins could help by providing an in-depth reflection on CPSs throughout their lifecycle to enable continuous monitoring and documentation of security aspects.

1.7. Summary of good technical practices in cybersecurity

Security must also be addressed through appropriate technical capabilities and environments where they are deployed (ANSSI 2014; ENISA 2018).

This section will outline what we consider to be cybersecurity guidelines for Industry 4.0.

Table 1.7 summarizes these practices proposed by the ANSSI. For each practice, the following details are presented:

– the reason why it must be taken into account;

– the application method;

– its perimeter (hardware, networks, infrastructure, etc.);

– the application-related constraints;

– how to manage these constraints.

However, some IoT- and smart manufacturing-related metrics are missing. For this reason, they will be presented in detail in the following sections.

1.7.1. *Trust and integrity*

This practice makes it possible to guarantee data and device integrity and reliability. The following measures must be applied:

– verify software integrity and source before running it;

– for IoT devices, authorize them within the network using digital certificates/PKI;

Pratice	Motivation	Method	Perimeter	Constraints	Constraint management mechanisms
Physical access point control	Determine the system entry points	Identify access (Who? What for? How often?), protect servers, equipment, cable access (computer rooms, locked cabinets)	Workstations, servers, network devices, machines, touch screens	System size, maintain access even in an emergency	Alarmed door “dry contact”, break glass procedures
Network segregation	Limit attack propagation and contain vulnerabilities	Establish a flow map, filter, trace and separate the network with VLANs	Networks (SCADA, PLC, development, etc.)	Real-time constraints (process networks)	Filtering applied upstream, physical access control to network equipment
Mobile device management	Reduce the risk of malware attacks with portable media (USB, HDD, etc.)	Define the policy, software restrictions, restrict use of this media, USB ports	Workstations, servers, consoles, touch screens	Need to exchange data between non-interconnected networks	Clean machines (strengthened, secured) for data transfers
Account management	Protect from unauthorized access	Account policy (users/applications), no default logins, strong passwords changed regularly	OS, databases, applications (SCADA/PLC), network devices, machinery	Generic accounts, emergency access	Traceability actions, strict procedures to determine identity with generic accounts (moment-by-moment)

Pratice	Motivation	Method	Perimeter	Constraints	Constraint management means
Configuration hardening	Restrict areas exposed to attacks	Install only necessary software, protocols and services, avoid default options, disable vulnerable protocols	OS, applications (SCADA/PLC), network devices, touch screens	Impact of alterations on production applications	Documented analysis, exception management for necessary non-secured features
Monitoring, warnings and alerts	Intrusion detection, action tracking, maintenance interventions	Enable traceability mechanisms (syslog, Windows events, etc.), filter and generate alerts for relevant events	OS, databases, network equipment, PLC, etc.	High volume of generated logs	Event management tools (filter, restrict, delete, etc.)
Configuration management	Ensure that there are no malicious modifications between versions	Comparison between running applications and reference application configuration, identify variations before deployment	Apps (SCADA/PLCs), network devices (configuration files)	ICSs complexity and heterogeneity	Configuration management tools to identify variations between two versions

Practice	Motivation	Method	Perimeter	Constraints	Constraint management mechanisms
Backup and restoring	Data must be available in case of full reboot after an attack or incident	Backup policy (which data should be backed up for users or according to regulatory requirements?)	Source codes, databases, logs, PLC firmware, network equipment configs (switches, routers, etc.)	Backup cannot be automatically performed for some devices (sensors, actuators for PLCs)	Track changes in settings, control, adjustments, sensor/actuator alarms
Documentation	Keep accurate system representations and control information dissemination	Documentation policy (update process, storage duration, etc.)	Factory, architectural plans, locations, administration and maintenance manuals, system analysis, etc.	Hard copies of documents may contain passwords (constraint), their control is complicated	Inform users of the risks with documentation, no document can be seen on the desktop
Malicious code detection	Advanced protection against virus attacks	Protection policy, priority to equipment/applications directly connected with the outside world and users	SCADA applications, engineering stations, programming and maintenance consoles	Incompatibility with older applications, no antivirus update, contractual issues (loss of warranty)	Deploy antivirus on handheld and maintenance machines, configuration hardening

Practice	Motivation	Method	Perimeter	Constraints	Constraint management mechanisms
Upgrade and patch management	Preventive protection against attacks, bug-related outages, vulnerabilities	Constraint-adapted patch management policy (systematic or periodic), identified risks and hardware	OS, applications, firmware, operator machines, servers, PLCs, telecom equipment, touch screens	Patches should be evaluated before deployment, some devices are not easily shut down	Identify vulnerabilities, schedule updates, monitor traffic, harden configurations and isolate devices
PLC protection	PLC program protection	PLC protected access (passwords), source code, read-only access for first-level maintenance, PLC cabinet locks	Production PLC, PLC programs	-	-
Engineering and development stations	Vulnerability points and contamination vectors (handhelds, connection to other networks)	Patches, antivirus software, no non-SCADA connection, usage monitoring, shutdown when not in use	SCADA development stations, PLC console, handheld devices for sensor and actuator configuration	-	-

Table 1.7. *Good cybersecurity practices for Industry 4.0*

– define secure data exchange channels for IoT devices (whitelist);

– implement application whitelists and periodic (annual) review of the list when changes occur;

– use cryptography mechanisms to ensure production data integrity;

– monitor data at rest and in transit to detect unauthorized modifications.

1.7.2. *Cloud security*

Security aspects of cloud computing are concerned by this practice. The following measures must be applied:

– choose the cloud type according to the company, the impact on privacy, the laws and the cloud provider's country;

– insert security and availability aspects in the agreements with cloud providers;

– avoid single point of failure with cloud applications and centralized systems;

– determine critical systems and applications when using public clouds;

– to minimize risk of cloud attacks, use a zero-knowledge approach and protect all data in the cloud and during transfer.

1.7.3. *Machine-to-machine safety*

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

– use an HSM server in the infrastructure to store the service layer keys in the long term;

– establish a security association between communicating entities and cryptographic algorithms to ensure mutual authentication, integrity and confidentiality;

– use communication protocols capable of detecting unauthorized repetition of previous messages;

– for protection against cross-site scripting and command injection, use whitelist entry validation.

1.7.4. *Data protection*

Data protection is a very general concept, but in this case, it is related to the guarantee of data privacy at different levels within a company and managing access to data. The following measures must be applied:

– protection of data at rest (volatile and non-volatile memory), in transit and in use;

– data categorization based on risk analysis, criticality assessment and definition of security measures;

– grant access to specific data to third parties with least privileges and document this access;

– for highly confidential 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.

1.7.5. *Software/firmware updates*

Just as with any other device, software updates with IoT solutions must follow a specific methodology, whose measures are:

– ensure strict update control (no modifications between the source and the destination);

– only deploy patches after testing and proving that there are no negative consequences;

– for systems that cannot be updated, compensatory measures must be applied.

1.7.6. *Access control*

IoT devices are critical devices in Industry 4.0 and can be physically or remotely accessed. For this reason, the following access control measures must be applied:

– minimum authentication and authorization level for given system segments;

– implementation of multi-factor authentication;

– application of the principle of least privilege;

– implementation of an account lockout feature;

– remote access segregation;

– physical access security must be taken into consideration.

1.7.7. *Networks, protocols and encryption*

Proper protocol implementation, encryption and network segmentation are key elements for building a strong IoT network. The following actions are linked to this objective:

– use secure communication and encryption channels when possible;

– use proven standards-based protocols (TLS 1.3) and avoid vulnerable protocols (Telnet, SNMP v1/v2);

– limit the number of protocols in a given environment and disable unused services;

– ensure security capabilities and interoperability between protocols.

1.7.8. *Monitoring and auditing*

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

– implementation of a passive monitoring solution to create a baseline of industrial network traffic;

– real-time security log analysis using SIEM solutions (Security Information and Event Management);

– periodic log, access privilege and configuration reviews;

– real-time availability monitoring of IoT devices.

1.7.9. *Configuration management*

The IoT encompasses a wide range of devices; it is important to keep track of changes in configurations, device hardening and backup methods.

The following measures are in line with this goal:

– basic customized security configurations for different types of assets;

– documentation of any configuration changes in accordance with the change management policy of the organization;

– implementation of support tools for configuration management;

– creation of a complete backup plan, adapted to the different types of assets.

1.8. Industry 4.0, cybersecurity and traceability outlines

In this chapter, we have explored cybersecurity concepts and solutions within the context of Industry 4.0 through scientific and normative literature. In the analyzed articles, certain aspects of cybersecurity were not always mentioned, such as the managerial aspect of cybersecurity or the business impacts (Zia et al. 2022). For this reason, our study was structured as a step-by-step approach to provide a comprehensive overview of the topic. In addition to being an introductory review of scientific work on cybersecurity, it can also be used as a guide to introducing cybersecurity into a smart manufacturing environment.

After introducing the concept of Industry 4.0, we showed the complexity created by cybersecurity mechanisms to ensure system security, due to the many innovative technologies involved.

We then proposed a characterization of cybersecurity in terms of both its technical and managerial aspects to show that every level in an organization has a role to play. Given that cybersecurity must be considered in terms of physical zones, we proposed a division of a factory into several perimeters, which we characterized according to their interactions, equipment and networks. We then outlined the cybersecurity vulnerabilities, threats and risks met in Industry 4.0 factories for each perimeter, while taking into account the business impacts at the organizational level (Figure 1.12).

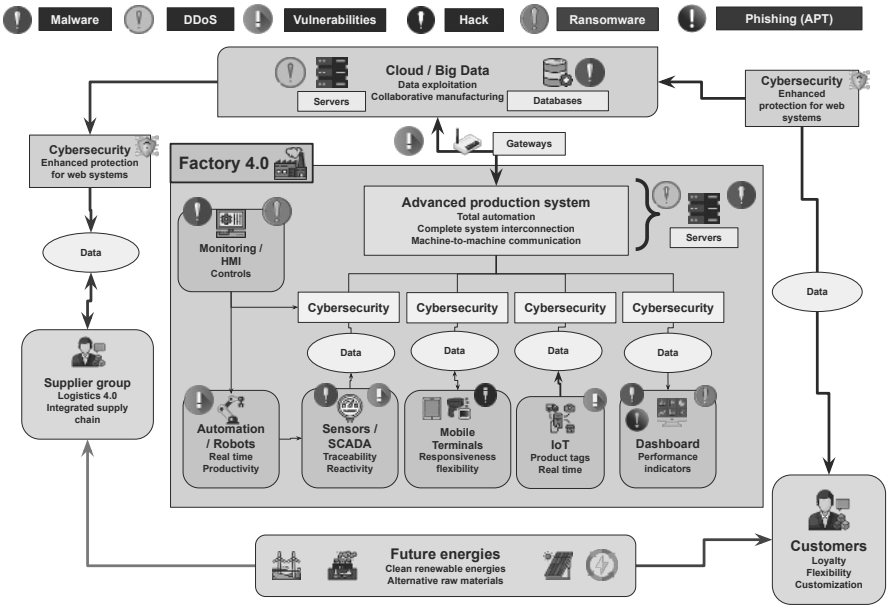

Figure 1.12. *Cybersecurity risks overview in a factory 4.0*

On the one hand, connecting the factory to the Internet in order to enable real-time information transmission and sharing with the outside world will result in the creation of a gateway between networks, which may give rise to new security breaches. On the other hand, the factory devices each exhibit their own risks in terms of cybersecurity (mobile devices can be hacked, the IoT has vulnerabilities, servers are prone to DDoS, etc.). Among these new technologies, some are closely related to the notions of product identification and traceability in the factory (sensors, IoT, RFID tags, etc.).

It can be seen that Factory 4.0 will be managed by data from different sources, both internal and external. With the help of outsourced storage through big data and the Cloud, the factory will be able to manage all the data related to a product, from its design to its end of life, from its production to its marketing, and be able to keep them for as long as necessary. Most importantly, the factory will need to be able to retrieve, integrate and leverage data created by the industry in general and its customers in particular. Once all these data have been compiled, it will be able to infer a consistent predictive analysis. Chapter 2 will address the topic of the operational management of the part of this mass of data created by the traceability system.

1.9. References

Abu Jassar, A., Attar, H., Yevsieiev, V., Amer, A., Demska, N., Luhach, A., Lyashenko, V. (2022). Electronic user authentication key for access to HMI/SCADA via unsecured internet networks. *Computational Intelligence and Neuroscience*, 2022(1), 1–13.

Alani, M. and Alloghani, M. (2019). *Security Challenges in the Industry 4.0 Era*. Springer, Berlin.

Alcácer, V. and Cruz-Machado, V. (2019). Scanning the industry 4.0: A literature review on technologies for manufacturing systems. *Engineering Science and Technology, an International Journal*, 22(3), 899–919.

Ali, A., Shah, G., Farooq, M., Khan, M.U. (2017). Technologies and challenges in developing machine-to-machine applications: A survey. *Journal of Network and Computer Applications*, 83, 1–13.

Alqudhaibi, A., Albarrak, M., Jagtap, S., Williams, N., Salonitis, K. (2025). Securing Industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management. *Cyber Security and Applications*, 3, 100067.

ANSSI (2014). Managing cybersecurity for industrial control systems. Report, ANSSI.

Asghar, M.R., Hu, Q., Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, 165, 106946.

Ashton, K. (2009). That 'Internet of Things' thing. *RFiD Journal*, 22, 97–114.

Atzori, L., Iera, A., Morabito, G. (2016). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56, 122–140.

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security*, 89, 101677.

Brandao, P. and Duarte, P. (2022). Cybersecurity risk management in the Industry 4.0. *International Journal of Scientific Research And Growth*, 9, 661–668.

Carcano, A., Coletta, A., Guglielmi, M., Masera, M., Nai Fovino, I., Trombetta, A. (2011). A multidimensional critical state analysis for detecting intrusions in scada systems. *IEEE Transactions on Industrial Informatics*, 7(2), 179–186.

Corallo, A., Lazoi, M., Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, 114, 103165.

Dawson, M. (2018). Cyber security in Industry 4.0: The pitfalls of having hyperconnected systems. *Journal of Strategic Management Studies*, 10(1), 19–28.

Eckhart, M. and Ekelhart, A. (2019). *Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook*. Springer, Berlin.

ENISA (2018). Good practices for security of Internet of Things in the context of smart manufacturing. Report, ENISA.

European Commission (2021). Industry 5.0 – Towards a sustainable, human-centric and resilient European industry [Online]. Available at: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-towards-sustainable-human-centric-and-resilient-european-industry_en.

Fernández-Caramés, T.M., Fraga-Lamas, P. (2019). A review on the application of blockchain to the next generation of cybersecure Industry 4.0 smart factories. *IEEE Access*, 7, 45201–45218.

Flaus, J.-M. (2019). *Cybersecurity of Industrial Systems*. ISTE Ltd, London and Wiley, Hoboken, NJ.

Geandarme, F. (2018). Industrie 4.0 : définition et mise en œuvre vers l'usine de production connectée [Online]. Available at: https://www.visiativ.com/actualites/actualites/industrie-4-0-definition-et-mise-en-oeuvre-vers-lusine-de-production-connectee/.

Graham, J., Hieb, J., Naber, J. (2016). Improving cybersecurity for industrial control systems. In *Proceedings of the 2016 IEEE 25th International Symposium on Industrial Electronics (ISIE)*, Santa Clara, CA.

Haleem, A., Javaid, M., Singh, R., Rab, S., Suman, R. (2022). Perspectives of cybersecurity for ameliorative Industry 4.0 era: A review based framework. *Industrial Robot*, 49(3), 582–597.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*, 7, 82721–82743.

Illési, Z., Halász, A., Varga, P.J. (2018). Wireless networks and critical information infrastructure. In *Proceedings of the 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. Forschungsunion, Acatech, Munich.

Kagermann, H., Wahlster, W., Helbig, J. (2013). Recommendations for implementing the strategic initiative Industrie 4.0 [Online]. Available at: https://www.din.de/resource/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf.

Kiss, M., Breda, G., Muha, L. (2019). Information security aspects of Industry 4.0. *Procedia Manufacturing*, 32, 848–855.

Kondiloglu, A., Bayer, H., Celik, E., Atalay, M. (2017). Information security breaches and precautions on Industry 4.0. *Tehnologčnij Audit ta Rezervi Virobnictva*, 64(38), 58–63.

Lezzi, M., Lazoi, M., Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, 103, 97–110.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5), 1125–1142.

Liu, H. and Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences*, 9, 4396.

Lu, T., Guo, X., Li, Y., Peng, Y., Zhang, X., Xie, F., Gao, Y. (2014). Cyberphysical security for industrial control systems based on wireless sensor networks. *International Journal of Distributed Sensor Networks*, 10(6), 438350.

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A., Maniatakos, M., Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5), 1039–1057.

Miraz, D., Ali, M., Excell, P., Picking, R. (2015). A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In *Proceedings of 2015 Internet Technologies and Applications (ITA)*, Wrexham, 219–224.

Mitchell, R. and Chen, I. (2013). Behavior-rule based intrusion detection systems for safety critical smart grid applications. *IEEE Transactions on Smart Grid*, 4(3), 1254–1263.

Mozzaquatro, B.A., Jardim-Goncalves, R., Agostinho, C. (2015). Towards a reference ontology for security in the Internet of Things. In *Proceedings of the IEEE International Workshop on Measurements Networking*, Coimbra, 1–6.

Mozzaquatro, B.A., Agostinho, C., Goncalves, D., Martins, J., Jardim-Goncalves, R. (2018). An ontology-based cybersecurity framework for the Internet of Things. *Sensors*, 18(9), 3053.

Mullet, V., Sondi, P., Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access*, 9, 23235–23263.

Nunes, B.A.A., Mendonca, M., Nguyen, X., Obraczka, K., Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys Tutorials*, 16(3), 1617–1634.

Omari, A., Alsariera, Y., Alhadawi, H., Albawaleez, M., Alkhliwi, S. (2022). A closer look on challenges and security risks of voice over internet protocol infrastructures. *IJCSNS*, 22, 175.

Ozarpa, C., Avci, I., Eldekçi, A. (2022). Industry 4.0 and cybersecurity at automobile manufacturing in smart factories [Online]. Available at: https://www.researchgate.net/publication/360836993_Industry_40_and_Cybersecurity_at_Automobile_Manufacturing_in_Smart_Factories_Akilli_Fabrikalardaki_Otomobil_Imalatinda_Endustri_40_ve_Siber_Guvenlik.

Pan, Y., White, J., Schmidt, D., Elhabashy, A., Sturm, L., Camelio, J., Williams, C. (2017). Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems. *International Journal of Interactive Multimedia and Artificial Intelligence*, 4, 45–54.

Pereira, T., Barreto, L., Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, 13, 1253–1260.

Petrenko, S. (2020). *Developing a Cybersecurity Immune System for Industry 4.0*. River Publishers, London.

Prinsloo, J., Sinha, S., von Solms, B. (2019). A review of Industry 4.0 manufacturing process security risks. *Applied Sciences*, 9(23), 5105.

Rahman, Z., Yi, X., Khalil, I. (2022). Blockchain based ai-enabled Industry 4.0 CPS protection against advanced persistent threat. *CoRR*. doi: 10.48550/arXiv.2201.12727.

Reinsel, D., Gantz, J., Rydning, J. (2018). The digitization of the world from edge to core. Report, Seagate.

Rubio, J.E., Alcaraz, C., Roman, R., Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers and Security*, 87, 101561.

Rudenko, R., Pires, I., Oliveira, P., Barroso, J., Reis, A. (2022). A brief review on Internet of Things, Industry 4.0 and cybersecurity. *Electronics*, 11, 1742.

Satasiya, D. and Raviya Rupal, D. (2016). Analysis of software defined network firewall (SDF). In *Proceedings of the 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, Chennai, 228–231.

Sawik, T. (2020). A linear model for optimal cybersecurity investment in Industry 4.0 supply chains. *International Journal of Production Research*, 60(4), 1368–1385.

Shukla, M., Sarmah, S., Tiwari, M. (2022). A multi-objective framework for the identification and optimisation of factors affecting cybersecurity in the Industry 4.0 supply chain. *International Journal of Production Research*, 61(15), 5266–5281.

Sicard, F., Zamai, É., Flaus, J.-M. (2018). *Critical States Distance Filter Based Approach for Detection and Blockage of Cyberattacks in Industrial Control Systems*. Springer, Berlin.

Sicard, F., Zamai, E., Flaus, J.-M. (2019). An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems. *Reliability Engineering and System Safety*, 188, 584–603.

Tange, K., De Donno, M., Fafoutis, X., Dragoni, N. (2020). A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities. *IEEE Communications Surveys Tutorials*, 22(4), 2489–2520.

Thames, L. and Schaefer, D. (2017). *Cybersecurity for Industry 4.0 and Advanced Manufacturing Environments with Ensemble Intelligence*. Springer, Berlin.

Tsuchiya, A., Fraile, F., Koshijima, I., Ortiz, A., Poler, R. (2018). Software defined networking firewall for Industry 4.0 manufacturing systems. *Journal of Industrial Engineering and Management*, 11(2), 318–333.

Wegner, A., Graham, J., Ribble, E. (2017). *A New Approach to Cyberphysical Security in Industry 4.0*. Springer, Berlin.

Whitmore, A., Agarwal, A., Xu, L. (2014). The Internet of Things – A survey of topics and trends. *Information Systems Frontiers*, 17, 261–274.

Wolf, M. and Serpanos, D. (2018). Safety and security in cyber-physical systems and Internet-of-Things systems. *Proceedings of the IEEE*, 106(1), 9–20.

Zeng, P., Wang, Z., Jia, Z., Kong, L., Li, D., Jin, X. (2019). Time-slotted software-defined industrial ethernet for real-time quality of service in Industry 4.0. *Future Generation Computer Systems*, 99, 1–10.

Zhao, G., Zhang, C., Zheng, L. (2017). Intrusion detection using deep belief network and probabilistic neural network. In *Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, 639–642.

Zia, N., Burita, L., Huseynova, A., Owusu, V. (2022). A managerial review and guidelines for Industry 4.0 factories on cybersecurity. *European Conference on Cyber Warfare and Security*, 21, 336–340.