applied sciences

MDPI

Review

Security Challenges in Industry 4.0 PLC Systems

Janusz Hajda, Ryszard Jakuszewski and Szymon Ogonowski *

Department of Measurements and Control Systems, Silesian University of Technology, Akademicka 16, 44-100 Gliwice, Poland; janusz.hajda@polsl.pl (J.H.); ryszard.jakuszewski@polsl.pl (R.J.)
* Correspondence: szymon.ogonowski@polsl.pl

Abstract: The concept of the fourth industrial revolution assumes the integration of people and digitally controlled machines with the Internet and information technologies. At the end of 2015, more than 20 billion machines and devices were connected to the Internet, with an expected growth to half a trillion by 2030. The most important raw material for this digital revolution is data, which when properly stored, analyzed and secured, constitute the basis for the development of any business. In times of rapid industrial development, automation of production processes and systems integration via networks, the effective protection of the cyber-physical systems of a plant is particularly important. To minimize the risks associated with Internet access, one must define all the possible threats and determine their sources in the plant and block or minimize the possibility of sabotage or data loss. This article analyzes the security measures used in industrial systems. In particular, risk management and the study of the risk sources in terms of human, hardware and software aspects in networked PLC and SCADA systems are discussed. Methods of improving the architecture of industrial networks and their management are proposed in order to increase the level of security. Additionally, the safety of the communication protocols with PLCs in industrial control systems is discussed.

Keywords: industry 4.0; cybersecurity; cyber-physical system; PLC network; communication; risk management

Citation: Hajda, J.; Jakuszewski, R.; Ogonowski, S. Security Challenges in Industry 4.0 PLC Systems. *Appl. Sci.* **2021**, *11*, 9785. https://doi.org/10.3390/app11219785

Academic Editors: Dariusz Kania, Robert Czerwiński and Paula Fraga-Lamas

Received: 9 September 2021
Accepted: 18 October 2021
Published: 20 October 2021

1. Introduction

The beginning of the first industrial revolution is dated as from the end of the 18th century and was driven by mechanical production plants based on steam power. At the beginning of the 20th century, there was a second revolution based on mass labor production using electrical energy. Then the third industrial revolution began in the 1970s and was driven by automatic production based on electronics and internet technology. Nowadays, the fourth industrial revolution, namely Industry 4.0, is happening. The idea of Industry 4.0 was initially proposed as a means of developing the German economy in 2011 [1–7].

The fourth industrial revolution places increasing expectations on governments resulting from the new role of the state in the economy and its involvement in solving problems of unreliable markets [8], with the key issue being the management and effectiveness of the state's activities, rather than the state size. Industrial policy being implemented by many countries is de facto aimed at reorienting national economies towards a fourth generation of industry [9], be it with a view to preserving and restoring jobs or by trying to improve competitiveness and added value of domestic production. The possible benefits are not only an improvement in efficiency, a reduction in errors, lower demand for raw materials and cost reduction, but also an opportunity to sell your own solutions to cooperators and clients. Transformation towards Industry 4.0 in the long run will bring measurable effects in the form of a higher rate of return on the invested company capital [9]. The road to reach such goal is, however, very difficult, following from the nature of the Industry 4.0 concept. Such transformation imposes not only technological challenges but also organizational [10,11] and sociological [12–14] ones.

While aiming to achieve a higher level of automatization and operational productivity [15], the Industry 4.0 concept requires vast computerization, inter-connection and horizontal and vertical integration in the traditional industry [4]. Production in Industry 4.0 can be treated as a cyber-physical system (CPS) [16,17] based on heterogeneous data and knowledge integration [4,6]. CPS is defined as a set of transformative technologies for managing interconnected systems between its physical assets and computational capabilities [18]. It creates an interoperable, optimized adaptive and scalable manufacturing process that is usually service-oriented [19]. It allows for an intelligent flow of produced elements between machines in a factory with real-time communication between machines [20]. Such systems require and are based on new technologies (see Figure 1), such as the Internet of Things (IoT) [21–28] and Services (IIoS) [29,30], Big Data (BD) [31–33], Edge/Fog/Cloud Computing [34–43], Blockchain [44–48], Industrial Automation, Cybersecurity [49,50], Intelligent Robots and Cobots [51–53].

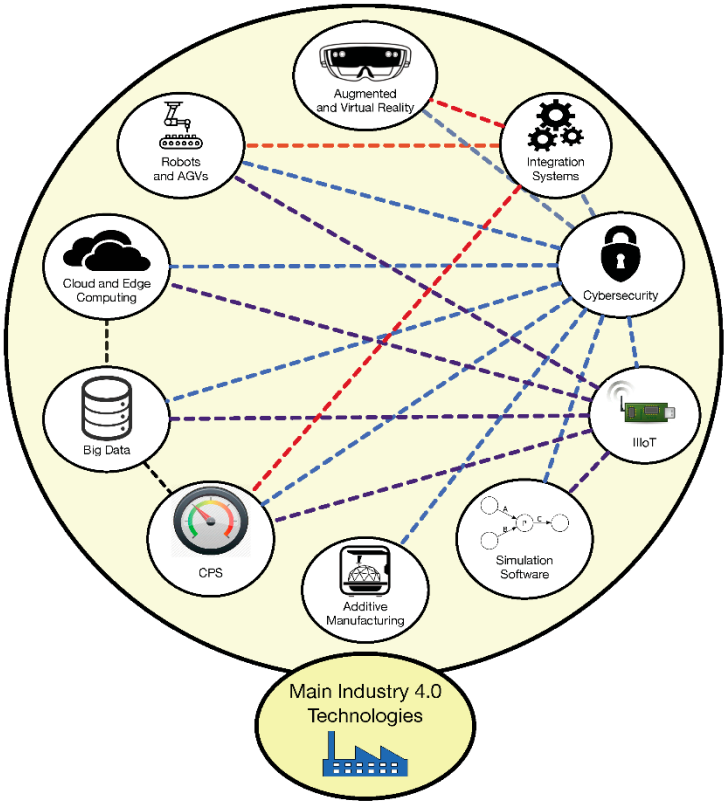

Figure 1. Main technologies of Industry 4.0 [54].

All the technologies mentioned above are essential for achieving the desired benefits of adopting Industry 4.0 in factories and in the whole value production chain. Application of such technologies requires, however, tight integration using networking solutions. This is why Industry 4.0 will face traditional cybersecurity issues and some other new ones following the nature and scope of the systems integration. If these solutions are not addressed properly, the true potential of the new industrial revolution may never be achieved. The most significant challenge related to cybersecurity is the integration and cooperation amongst the stakeholders of any given Industry 4.0 organization. All participating environments are made of diverse technologies spread across many disciplines with many different types of subject-matter experts; however, there are few standards and processes designed to assist each entity to communicate with respect to the high standards of cybersecurity [55]. Moreover, even if we take a more narrow range, namely, only inside one entity (e.g., production factory), the complexity of security problems does not scale down significantly. The multilayered structure of the control and management systems

and multi-objective tasks performed by these systems often require different standards of hardware and software with different cybersecurity requirements [56]. Usually, the physically controlled access to the plant is sufficient enough to secure the intranet network. While this was true in most cases, it is definitely not enough for Industry 4.0 solutions. In this paper, the security challenges of the transformation to the Industry 4.0 standards are discussed with a strict focus on PLC systems. While other solutions based on new technologies are supposed to be the core of the I4.0 factories, PLC-based systems still will be required and essential in most of the solutions [57,58]. In Section 2, the paper will discuss the overall risk management with the vulnerabilities and threats identification, followed by the existing security assessment. Section 3 will describe known risk sources in Operational Technology (OT) [59,60] systems with several examples of these systems' vulnerabilities exploitation. Section 4 will discuss where the most urgent actions are required in industrial control network systems, presenting several examples of solutions improving the security. All the presented examples of threats, vulnerabilities and mitigation methods follow from the literature review and from the professional experience of the authors in designing and commissioning PLC-based control systems in various industry branches. The presented cases are meant to show the extent of the challenges regarding security in Industry 4.0 PLC systems.

2. Risk Management

Lack of awareness of the dangers of unauthorized access to the industrial network may have significantly negative consequences for the functioning of the enterprise [61–63]. It lowers the level of availability of network resources and their reliability, and may cause significant difficulties in ensuring the safety of employees as well as damage the industrial installations and security of information of the production process [64]. In turn it generates financial losses for the enterprise, affects reputation on the market as well as decreases competitiveness caused by the outflow of information.

The key question that owners and integrators of industrial environment should ask is whether a given network has the correct architecture and whether it is properly secured against unwanted external interference. Constantly ensuring the security of industrial infrastructure becomes an increasing challenge. Until recently, the requirements for people securing elements of industrial automation were quite low, even marginal, due to the separation of machines from IT networks and the clear allotment of the rights of selected employees to change the parameters or software of a certain unit. Currently, in the era of Industry 4.0, the requirements for securing industrial infrastructure are much more extensive.

Efficient and effective cybersecurity risk management requires identification of key services and assets, identification of threats and vulnerabilities, assessment of existing security measures, risk analysis, determination of actions necessary to minimize the effects or lowering the probability of a network incident, continuous risk monitoring and reporting on potentially dangerous situations. The main challenges related to the above activities are presented in the sections below.

2.1. Key Assets and Services

The first stage of effective cybersecurity risk management is to identify the services and assets that are key to the proper operation of the enterprise. This is the stage that allows to determine the places in the enterprise that require the best protection in view of their impact on the operation issues. Tracing all the most important elements related to the safe operation of the enterprise is then required. Key assets and services are different and depend on business, location and access to media. Considering cybersecurity, however, the assets should be limited to resources of a certain value, related to the network infrastructure or stored in the company's network, and having an impact on its economic performance. Among the most important and most common company assets in the context of cybersecurity, we can distinguish the following:

- The production process diagram;
- Settings related to the production process and recipes;
- Sensitive employee data;
- The type and quantity of materials used in the production process;
- Current production status;
- List of customers and their demands.

The protection of the production process and the related settings and recipes is of the obvious importance for the company. Nobody questions the importance of protecting customer base. Often, however, when determining the assets of the enterprise, an important element—the employees' data—is not taken into account. The employees' competences and their personal data are as important as the list of clients. This is mainly due to two factors. The first is the possibility of the appropriate use of the employee due to his competences, and thus generating potentially more income. If these data were obtained by competitors, better qualified employees could be stolen in order to weaken the enterprise. The second factor is one of the repercussions related to the improper management of sensitive employee data under the General Data Protection Regulation of 10 May 2018 (GDPR) [65].

Among the most common key services in the context of cybersecurity of industrial networks, one may distinguish essentially one unchanging element, which is secure and constant access to the external and internal tele-information network, as well as services provided as part of this access (e-mail, network drives and network applications).

2.2. Identification of Threats and Vulnerabilities

The greatest threat to the industrial network of a plant is humans. The number of real-life examples serve as proof. The most common method of hacking into a company's network is taking over the employee's authorization path (login and password) [66]. Technological issues and the industrial process itself are also important. The more dispersed the network structure, the more potential points of unauthorized access to it. Therefore, from the point of view of cybersecurity risk analysis, the designed security should be matched to industrial technologies and their architecture [67].

First of all, the scope of the industrial network that will be taken into account when identifying the risk should be determined. This is a factor depending on the initial network fragmentation, especially if the production plant has machines that use different software standards or different data transmission methods. The most frequently used techniques for identifying risks related to cybersecurity of industrial networks include:

- Verification of machine documentation along with their communication and software standards. This method is aimed at verifying whether the communication standards used are protected against hacker attacks and whether the software of the machines is up-to-date and properly secured. In addition, a physical verification is performed whether all elements are compliant with the electrical documentation or they may have been replaced (e.g., during a breakdown) with a newer model offering up-to-date software.
- Verification of the management of the architecture and network sections is aimed at checking whether all security standards defined during the creation of the network are maintained and properly managed by authorized persons.
- Interviews with production plant employees responsible for the operation of machines and the security of the industrial network. Thanks to this method, it is possible to obtain information on security incidents or to obtain valuable information related to accidentally found errors in network configurations.
- Verification of the management of special parts of the network and special devices active in the network. This applies to devices essential for the operation of the enterprise, which do not need to be directly and permanently connected to the industrial network.
- The analysis of the configuration and settings in active network devices assumes the validation of the data entered into these devices. Additionally, this method checks

that the software offered by the manufacturer for the given devices is up to date in order to ensure a better level of security.

- Monitoring the operation of devices responsible for security and verification of logs. This method consists of connecting devices operating in the 'Man in the Middle' mode, allowing the collection of an information packet without editing the data packet in order to track whether any of the devices intentionally modifies the signal or distorts it. Verification of device logs allows to see previous incidents related to the security of the industrial network.
- Physical checking of security effectiveness during controlled attacks. This is probably the most effective method identified by security reports. It consists of carrying out a series of controlled attacks inside an industrial network in order to find its vulnerabilities and adequately protect against external exploitation of these vulnerabilities.
- Port scan and network mapping to check robustness to network penetration. This method uses techniques related to the emulation of a given device in order to check the legitimacy and degree of authorization.
- Analysis of the network diagrams, production process, policy and procedures. Such analysis can show how the users are using the industrial network and whether their cybersecurity knowledge corresponds to their rights in the network.

When collecting a complete set of information on the state of the network security, special attention should be paid to people's awareness of cybersecurity, the condition and type of hardware of the network systems with their software as well as the security status of the network operating systems.

2.3. Assessment of Existing Security

The next step necessary to perform a proper risk analysis is the assessment of the already functioning security system. The process of validation of the security in the network systems is carried out in accordance with the threats for the defined industrial network defined in the previous stage. The assessment of functioning safeguards must always correspond to the actual threats.

Based on the technologies used to prevent security incidents and loss of data integrity in industrial networks, it is possible to determine whether the specified places pose a real threat. Since the discovery of the first computer worm in industrial network devices, many manufacturers have introduced a lot of mechanisms to ensure, for example, the integrity, confidentiality and availability of data, at least partially. At this step of the safety assessment, it should also be verified whether the implemented security elements work properly and on which parts specified in the risk identification they have a real impact. Determining the real impact should follow an input-to-output method, where the total information transmission path is examined, taking into account all locations where a cybersecurity attack may occur.

One of the methods that assess functioning security is the brute force method, where the main goal is to use awareness of a weak point in an industrial network in order to conduct a controlled attack aimed at verifying whether the existing security measures work properly. The assessment of functioning security should also include steps to validate the reporting of cybersecurity incidents. One should also check the place where the logs are saved and the appropriate security of access to these files. Reporting on potentially dangerous events has a significant impact on the security of the industrial network system due to the possibility of a quick response adapted to the level of threat.

2.4. Risk Analysis

The stage that allows to determine the significance of the threats and usefulness in the context of cybersecurity is an analysis combined with a risk assessment. The risk analysis usually concerns events for which the frequency of occurrence is not clearly defined or directly determined at an appropriate confidence level. For this reason, when performing a risk assessment, modeling methods adapted to estimating low probabilities, such as event

trees and error trees, are most often used. In the assessment of each risk, the complex task is broken down into simpler parts, which, after the analysis is performed, are combined again, obtaining a better understanding of the entire task, and thus the probability of the component events is determined.

The tree of events is a graphical way of presenting the dependence of causes and effects occurring in the problem of industrial networks cybersecurity. When building an event tree, it is assumed that the security incident is the result of a sequence of events. Thus, the event tree begins with an initiating event, and then presents all possible cause-effect sequences being its consequences. In many places of the event tree there are branching points where, after certain events, there is the possibility of various other potentially dangerous events. Thus, the probability of a specific effect is obtained by multiplying all successive probabilities of events that make up the path in the tree, along which the considered effect can be reached. The fault tree is also a graphical model of the cause–effect relationships, but it is built in the opposite direction to the event tree. This method begins with a specific effect and develops towards the events that precede it, while analyzing all possible combinations of adverse events that could have led to the analyzed effect. Event trees and fault trees can be used for both qualitative and quantitative cybersecurity analysis.

Using the probability determined in this way, it is possible to state the formula which estimates the risk [68,69]:

$$Risk = P(Vulnerability) \cdot P(Threat) \cdot P(Impact),$$

where $P(Vulnerability)$ is the probability of exploitation of a specific weak point, $P(Threat)$ is the probability of a specific threat occurrence and $P(Impact)$ is the probability of producing a specific effect. The risk is a function of the likelihood (probability) that a defined threat agent (adversary) can exploit a specific vulnerability and create an impact (consequence). In other words, cyber security risk is a function of the probability of a given threat source exploiting the known vulnerabilities and the resulting impact of a successful exploitation of the vulnerability [68,69].

The number of vulnerabilities in the above formula is defined as the number of known vulnerabilities in the unprotected cause–effect elements resulting from the tree structure; it is determined by counting individual points having a direct impact on the analyzed threat. The number of threats determines the number of points on the tree, which are the effects following the analyzed threat, and, in turn, the possibility of further exploitation of the examined point in the context of the spread of risk.

From an enterprise perspective, *Impact* is the most subjective element of this equation as it depends on the specific assets and underlying services that may be affected by an industrial network security incident. Most often it is defined on the basis of subjective assessments of material losses (economic losses) and damages related to human well-being (human resources), the reliability of the company or the quality of services offered. Due to different weights of factors, for each economic unit, an additional factor should be used in the formula to determine the impact in accordance with the priority of the production plant. After calculating the risk for each of the specified threats, it is possible to create a threat matrix containing a complete set of information related to the size of the risk and thresholds defining the levels of risk.

2.5. Risk Minimization

When carrying out the risk assessment process, it is important to remember that risks can be assessed and reduced, but cannot be eliminated. In practice, this means that regardless of the quality and quantity of funds used to eliminate the risk, there is no security implementation system that would guarantee 100% security of the information flow process. The process of lowering the probability and minimizing the effects of incidents related to the safety of industrial networks is closely related to the amount of resources at the disposal of an economic entity. The use of new technological solutions to prevent hacker attacks or the reconstruction of network infrastructure may turn out to be too expensive in relation to

the effect it is supposed to provide. Thus, it is necessary to validate and minimize the effort necessary to achieve the maximum acceptable level of risk. The most common activities aimed at reducing the probability and minimizing the effects of incidents related to the security of industrial networks include:

- Fragmentation of the industrial network—an activity based on the introduction or re-introduction of the original fragmentation of the network which uses of sub-networks, aimed at separating the set of business entity resources from access to the external network or limiting unauthorized access to individual active elements in the network.
- Introducing roles using access levels for users; determining roles for network users based on access levels adequate to the role played in the production plant. It makes possible to separate potentially dangerous units in the industrial network from accidental or intentional and unauthorized access to network resources.
- Updating of communication protocols. This problem mainly concerns production plants based on obsolete technologies, created mainly for trouble-free use while disregarding safety issues. The process of updating and replacing communication protocols usually requires considerable financial outlays, as in most cases it requires reconstruction of the network and hardware infrastructure.
- Upgrading hardware software of network systems. After worms and viruses are discovered, network hardware manufacturers most often patch system software. Updating this software in equipment operating in an industrial network is one of the most important elements reducing the risk of a hacker attack; however, according to a CyberX report [70], it is the most often overlooked.
- Exchange of technological solutions introducing high risks related to cybersecurity. As in the case of updating protocols, reconstruction of the network infrastructure and removal of technologically obsolete elements may be the only method to improve the level of security.

2.6. Risk Monitoring and Reporting

Each aspect of risk should be verified, and the risk analysis procedure must be repeated periodically due to the possibility of new threats arising over time with a real impact on the risk value. The risk monitoring process is aimed at preventing new, potentially dangerous situations that are related to the security of industrial networks. Depending on the internal arrangements of the economic unit, it is necessary to periodically monitor the security of the industrial network. This period should not be more than 24 months from the original risk analysis and not more than 12 months from the supplementary risk analysis in order to ensure the relative level of safety and the timeliness of the solutions applied [68].

Reporting is the next step to properly manage the risk. Unlike risk monitoring, which is a periodical process, reporting on potentially dangerous situations is an ongoing process. Effective reporting on new potentially dangerous situations is possible through the use of an internal warning system in the form of logs related to the industrial network cybersecurity. In addition, it is worthy to analyze the reports generated by information and communication (ICT) service providers and key service operators in order to identify threats that have a real impact on ensuring data integrity, confidentiality and compliance. Effective reporting and its appropriate analysis by a dedicated team allows for quick response to network incidents, which ultimately leads to an increase in the level of network security.

3. Risk Sources in OT Systems

In order to study the potentially dangerous parts of the networked industrial control systems, a detailed threat analysis is necessary by auditing the network infrastructure and malware that takes advantage of the weaknesses of these systems. Based on such an analysis, it is possible to define actions aimed at introducing a higher level of cybersecurity. The study of the places in industrial systems requiring the most urgent action is a very complex issue that mostly relates to the specific network infrastructure. Nevertheless,

three significant groups can be distinguished, which are of considerable importance in determining and identifying the risk associated with hacker attacks.

The first of the studied groups is the risk introduced by the so-called human component. The most common cause of attacks on industrial networks is an error related to failure to maintain network hygiene or the deliberate action of one of the employees of the company.

The second group considered during the analysis is the hardware of the network systems themselves. This group of devices includes elements such as controllers, routers and switches. When analyzing incidents and weaknesses related to network devices, it is also necessary to analyze the security of communication protocols between various elements in the network.

The last examined group of elements in the industrial supervision architectures is the software of the network systems and security of the communication between devices as well as defects in products offered by software producers that have a direct impact on the whole system security.

The following sections will discuss some of the most important aspects of system security with respect to the three groups mentioned above.

3.1. Human Component

People are introducing the broadest spectrum of industrial network cybersecurity risks for both intentional and unconscious reasons [71]. Computer networks are based on advanced technologies, but human error is one of the most common reasons for successful attacks by cybercriminals. According to the Data Breach Investigations Report 2020 (DBIR) [72] commissioned by Verizon, as much as 75% of data leaks due to the human factor were unconscious error of an employee, and 25% was the deliberate action of a person working in an industrial unit. Intentional data leaks caused by internal workers are much more dangerous and much harder to counteract against industrial systems due to the fact that awareness and knowledge of the production process is a key element of disguising the source of the threat. The methods and causes that most often threaten the security of data and industrial networks through unintentional human fault include phishing [73–75], cyber-physical attacks [76–78], low password strength and their duplication for private and corporate purposes [79]. This is why the cybersecurity trainings and rising awareness is one of the key aspects of eliminating the human component in risk sources [80].

Phishing is a method of acquiring data or sensitive information by impersonating another institution or organization. Most often, this type of attack is carried out by means of a message with a link to a fake page, resembling the original, on which the user enters the password and login. One can also distinguish another type of fraud through messages in which the fraudster impersonates a person with a higher degree in the enterprise in order to obtain data related to a specific production process. The term "whailing" is used to define extortion attempts against employees of the management board or higher-empowered groups exercising control over an economic unit.

Cyber-physical attacks are mainly based on threats to an employee who is ultimately to meet the demands of the scammer. The most common case of sending threatening messages together with requests for specific actions is a faulty employee mail filtering system.

Employee passwords and their proper management are a significant element of the security of industrial networks in the context of the human factor. The DBIR report clearly states that the main problem is the duplication of passwords by employees on private job portals, which makes the employee passwords available to hackers in the event of a data leak from one portal. In addition, the report highlights the wrong selection of the password level, indicating duplication of the login in the password field or entering the simplest combinations of numbers and digits.

3.2. Network System Hardware

Network devices are all devices that are connected to the industrial network to perform different tasks in the control system hierarchy (Figure 2). For the basic network infrastructure, one can distinguish active network elements (controllers, routers, switches, access points and servers) and passive elements such as signal cables and patch panels. Passive devices are units or network elements that carry the signal without processing; therefore, they do not pose a threat to the entire industrial network.

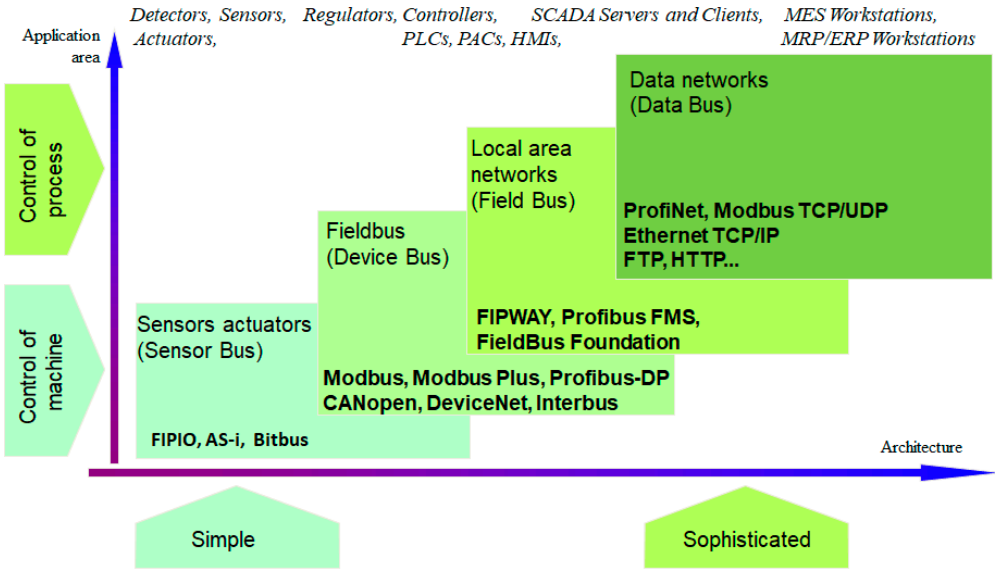

Figure 2. Location of the main industrial networks and buses—the areas of application overlap.

As active devices having a direct connection with the technical infrastructure of the plant (machines and devices on production lines), the most vulnerable to hacking attacks are programmable controllers and computers.

3.2.1. Security of the PLC Connection—Importance of the Network Architecture

The basic and one of the most overlooked threats in terms of the security of industrial networks is the connection between the PLC and the PC. This is an important topic for companies that have extensive networks of controllers located all over the factory. According to the CyberX report from 2019, based on the analysis of over 850 industrial networks, as many as 16% of manufacturing companies have wireless access points [70]. It often happens that the PLC is out of the reach of a qualified employee when diagnosing the cause of a failure in a program or when it is willing to modify its logic. Thus, many companies decide to use a wireless network for controller connection in order to carry out the required actions.

This solution is dangerous to the production process due to the lack of the PLC-level authentication for a person introducing changes in the logic of the controller. Even if the company uses password protection it is still of a basic level. In addition, poorly or incorrectly configured access points provide a large field for attacks via all types of devices equipped with a WiFi module. Access points equipped with gateways or advanced routers can also pose a risk to the enterprise. Such devices can be used by a complex data filtration software to intercept frames of popular protocols such as Modbus or ProfiNet, network mapping, or even establish a network redirection.

The connection of PLC controllers into one network with the general pool of IP addresses of all employees is also a significant threat. Such an architecture facilitates certain types of attacks, e.g., based on forcing outputs. The abovementioned CyberX report also shows that over 84% of the surveyed industrial networks have at least one external device

that allows remote connection to an internal industrial network. Thus, these enterprises for their own needs use access methods that reduce the security of the industrial network.

3.2.2. Routers, Access Points and Switches

Thanks to devices such as routers or switches, it is possible for machines to communicate with each other and connect them to a remote-control network. The task of these active network elements is primarily to ensure uninterrupted communication without data loss. The basic task facing industrial-grade equipment in the context of network security is verification of the person or device connecting. Appropriate verification and ensuring good network user authorization can significantly reduce the possibility of a MIM (Man in the Middle) attack. Appropriate verification can be performed by checking the hardware address of the device's network card, logging the user into the network and showing a special certificate during the connection. The most effective are methods that use combinations of authentication to join an industrial network. In addition, the appropriate use of routers and switches allows for network fragmentation, which makes it much more difficult for malware to search for devices during network mapping. It is also important to choose the right device depending on the size and degree of expansion of the corporate network so as to ensure uninterrupted data transmission with a stream of appropriate bandwidth. Routers and access points are the first network element to directly influence corporate cybersecurity attacks. Properly configured switches can significantly improve this security.

3.2.3. PLC Controllers

PLC controllers are one of the basic elements building industrial networks. They are electronic devices equipped with a microprocessor, designed to control the operation of a machine or technological device. A PLC controller is most often equipped with an appropriate number and type of input systems, the task of which is to collect information about the state of the object and operator's requests, as well as an appropriate number and type of output systems, whose task is to set the connected actuators and signaling elements or to handle data transmission.

The controller is adapted to a specific control task by means of the introduced operating algorithm, the main feature of which is the cyclicality of the program execution. At the beginning of each cycle, the controller downloads the input states and writes the value data to the appropriate registers in the memory. After executing all the commands and calculating the current state of the outputs, the controller transfers these states to the memory registers responsible for the controller outputs. Companies producing programmable controllers usually provide a programming environment that allows to write applications in one or more programming languages. These languages are usually a more or less precise implementation of the recommendations of IEC 61131-3.

As a network device, a PLC can be equipped with a module of data exchanging via the network with other controllers, and receiving or sending information to other devices active in the industrial network. With the knowledge of the structure and the basics of the operation of the PLC controller in a given process control system, it is possible to determine the conditions under which a given controller is connected to the industrial network. This is one of the key steps to identify locations vulnerable to cybersecurity attacks in a given industrial network.

Many people dealing with the security of industrial networks do not realize that the process control system is not completely isolated from the connection to the global network or assume that the risk of infection is negligible. It is true that ordinary computer viruses do not interact in any way with PLCs, but cybersecurity events suggest that controllers, such as SCADA systems, are at risk of being hacked even when isolated from the main industrial network with access to the global network.

In 2000, in Queensland, Australia, one of the former employees of a sewage treatment plant, using a computer, radio and commercially available software, took control of the

waste management system [81] for two months. His activity resulted in the release of over 800,000 L of untreated sewage into the environment. Another example confirming the importance of PLC security in industrial networks happened at the Davis-Besse nuclear power plant in Ohio, where in 2003 internal security was penetrated by malicious software [82]. As a result of this hacking attack, two important monitoring systems were disabled for almost 15 h. This type of accident in a nuclear power plant is particularly dangerous for human life, and it happened despite the strict rules established by federal law in the United States. In spite of the potentially serious risk of these cases, they were classified as a low-risk group, until 2010. The Stuxnet computer worm, the first known worm used to spy on and reprogram industrial installations has been identified and the topic of cybersecurity of industrial networks has been seriously dealt by PLC manufacturing companies and those responsible for network security. Despite its detectability in well-secured industrial networks, Stuxnet poses a serious threat as it opens the way for potential hackers to create new malware from its code to rebuild the algorithm in PLCs. Since 2010, many PLC manufacturers, such as Hitachi, Mitsubishi, Panasonic, Samsung and Siemens, have been working with antivirus software vendors (such as Kaspersky or Symantec) to find solutions to gaps and inefficiencies in PLC systems.

PLCs have been regularly used to build process control systems for over 40 years, but the concept of cyber-attacks and the steps to reduce them have been the subject of research for a relatively short time. Due to their susceptibility to hacking attacks, PLCs should be treated as ordinary personal or process computers. However, since the target of such attacks is the output of a physical process, the defined safety margins should be significantly increased. Below are some examples of ways to break security in installations based on PLCs:

Security of Communication Protocols

PLC controllers use different transmission protocols to communicate between field devices such as inverters, sensors or even devices for programming the controllers themselves in industrial networks. The most commonly used transmission protocols are MODBUS, Ethernet/IP, Profibus, DNP 317 and ISO-TSAP. These protocols offer efficient communication but were not designed to ensure transmission security in industrial systems because while developed, this problem was not considered to be an issue.

For this reason, the above data transmission methods do not ensure confidentiality and authentication, and in turn make the entire network vulnerable to various types of attacks.

Logic-Bypass Attack

Usually a PLC is equipped with two random access memory known as main and register memory. The main memory is used to store data of the program being executed, while the register memory is used as a temporary memory by the currently executing logic [83]. Despite the fact that the register memory is a temporary memory, it must contain some important variables that influence this logic. In general, from the level of computers located in the industrial network of the plant, there are no restrictions on access to the memory of PLC registers and on the free execution of read and write operations in this memory area. Therefore, it is enough to assume that a potential attacker has the ability to gain access to one device on the network and introduce a worm into the system, the purpose of which will be to enter random values into the PLC's registers. Since, as a result of the operation of such a worm, the register memory values will change, the parameters related to the operation of the logical part of the program may also change. Eventually, the logic, when executing the algorithm, will set a new value for the outputs based on random changes written to the registers, which can cause unpredictable results.

The Attack Based on the Output Forcing

The basic principle of PLC operation is to execute a specific program algorithm using the state of the inputs, and then, after completing all steps in the cycle, to update the outputs. Typically, for industrial systems based on a supervisory system (SCADA, HMI), PLCs have the function of a forced output setting. This allows the operator of the production process to remotely change the outputs of the control system despite the results of the control

algorithm, which can be achieved by direct connection to the PLC via an industrial network or by direct connection via the controller transmission port.

The process of forcing the output does not have any authorization verification mechanism, so virtually every person with access to the network where the controller is located can use this function. PLC outputs can affect the physical behavior of the process automation components, such as valves, switches, motors, etc. A person who wants to use this method does not need to have a lot of knowledge about the logic of the program. Considering the possibilities and the ease of carrying out this type of attack, it is not difficult to imagine the threat this poses to the production, plant and its employees.

LogicLocker

LogicLocker is a ransomware worm (ransom + software) that can hijack many PLCs from various popular manufacturers. The program is designed to bypass weak authentication mechanisms in PLCs. It blocks users while placing a "logic bomb" (a piece of code inserted into software to activate a malicious function under certain conditions) in the controller code. The attack method used in LogicLocker consists of five steps, as described below.

1. The initial infection usually takes place by taking advantage of security vulnerabilities. Since devices in industrial networks are typically always-on state, cybercriminals have enough time to break into a PLC, and controllers generally do not have strong authentication mechanisms that can help protect against a potential attack. The initial infection can take place when the user clicks on a malicious e-mail attachment or when visiting a crafted website.
2. After the initial infection, you can move horizontally (within the same OT subnetwork as presented in Figure 3a) or vertical (when switching between OT networks or from IT to OT networks as presented on the Figure 3b) to the PLC, which depends largely on how the controller is connected.
3. In the next step, the attacker blocks legitimate users to make system recovery difficult or impossible (e.g., by changing the password, overusing PLC resources, or changing the IP address of the controller). Different locking methods allow different degrees of success.
4. In the next stage, preparation for negotiations takes place, which consists of hiding the place of broadcasting the information. For this purpose, encryption or built-in functions of some controllers are used, e.g., the ability to send e-mails via a PLC.
5. Finally, negotiations are conducted between the cybercriminal and the victim in order to restore the correct operation of the system [84].

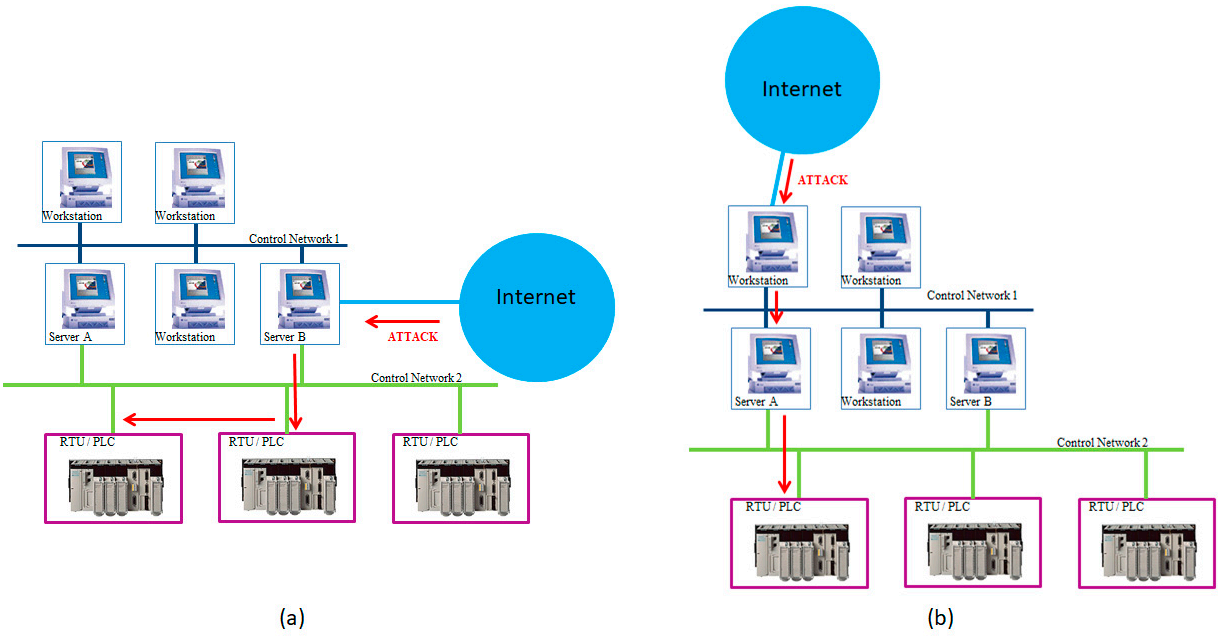

Figure 3. Two types of attack: (**a**) horizontal—between devices of the same subnetwork; (**b**) vertical—through subnets.

Attacks that Exploit the Weaknesses of the ISO-TSAP Protocol

Siemens Simatic S7 controllers are a group of controllers particularly exposed to hacking attacks and the use of their weaknesses due to their widespread use in industry and the use of the PROFINET network standard based on the modification of Industrial Ethernet.

Simatic TIA and Step 7 Engineering are used to program these controllers, and the communication between the software and PLC is based on the ISO-TSAP protocol standard. This protocol provides no encryption of the data exchanged between the PLC and the computer, which means that all data are transferred in clear text. The following are examples of attacks that exploit the weaknesses of the ISO-TSAP protocol:

- Response attack. The main assumption of this attack method is that the cybercriminal has the ability to intercept certain information or data and then use that data to later compromise the system. When analyzing the data transferred between the Step 7 software and the Simatic S7 controller, it is possible to distinguish certain elements of the frame that allow the analysis of the program logic, and even the physical process controlled by the PLC. The use of listening by an attacker may lead to the complete acquisition of data and analyze it, and then use this data to create its own command line sent to the controller.
- MIM attack (Man in the Middle). A weakness of communication using the ISO-TSAP protocol is the fact that the attacker has the ability to track the data stream between the PLC and the Step 7 software. Thus, the cybercriminal has the ability to collect a complete set of data exchanged between the software and the controller without being able to detect this fact. Information obtained in this way may significantly influence further attacks or lead to the exchange of erroneous data.
- Attack with authorization bypass. In some special cases, access to PLC may be password protected, but this is not a particularly popular practice in the industry due to the general belief that the industrial network is isolated from the global network. However, despite the password protection of the PLC controller, the cybercriminal has the possibility to bypass the verification due to the lack of any security of the ISO-TSAP communication protocol. So, if the attacker obtains an authorization package in the form of an encrypted password and login during a MIM attack, he may later use the same package when trying to authorize with the controller. In this case, the cybercriminal can easily use even the authorization data of another authorized user. In spite of the application and implementation of a user verification system with a password, it is not a method that gives real security effects.

PLC-Blaster

PLC-Blaster is a computer worm that was created to confirm the weakness of Siemens S7 drivers by a group of Black Hat hackers in 2016 [85]. This malware is special due to the fact that it does not require an additional PC to run. The system is infected by impersonating the worm as software for programming Siemens TIA-Portal controllers. Placed in one controller, the worm scans the network for other Siemens S7 PLCs that it could infect. Siemens Simatic controllers can be recognized by PLC-Blaster via port 102/tcp. No other service commonly used in industry uses this port, and its blocking is only possible through an external firewall. With each infection, the worm starts another scan for more PLCs from the freshly infected device. The worm executes along with the control program instructions through a function block added to the controller's memory. Overwriting the infected function block by the user removes the worm from a single controller in the industrial network. As a result of controller infection, PLC-Blaster can take control of the I/O system, modify the register memory and also perform shutdown or restart operations.

3.3. Software in Network Systems

The software of network systems is another element that has a significant impact on the security of industrial networks. When analyzing this issue, one should focus mainly on elements such as production process supervision systems, network operating systems and software managing active elements in industrial networks. According to the data

presented in the SANS report [86], as many as 4 out of 5 elements having the greatest impact on security are closely related to the subject of network systems software. The greatest doubts of people working on securing industrial networks are raised by the topic of secure connection with remote process control systems. There are several aspects of this, but undeniably the most important is the presence of viruses masquerading as supervision systems, such as Stuxnet, to manipulate variables in a PLC program and track the production process as a whole.

3.3.1. SCADA Systems

Supervisory Control and Data Acquisition (SCADA) are IT systems aimed at supervising the course of the technological or production process. The specific functions of the production process supervision systems include collecting current data from measuring elements, visualizing data, controlling the production process, alerting errors or deviations as well as data archiving using comprehensive databases. SCADA systems play a superior role in relation to the PLC controllers and other devices directly influencing the production process. PLCs either collect information directly from sensors or use devices that collect such data. Thus, via the controller, the data go to a computer system such as SCADA, where it is processed, visualized and archived. Process control system operators can set process parameters and often control the process in manual or emergency mode. It is also worth noting that SCADA systems are scalable and can process thousands of input variables, depending on the complexity and scope of the technology. Industrial supervision, control and data acquisition systems can communicate with the control layer devices via special industrial buses or networks in standards such as RS-232, RS-485, CAN or Profibus. However, more often, due to lower costs, classic computer networks based on Ethernet are used.

As in the case of PLC controllers (Section 3.2.3), one of the weakest points in SCADA are the protocols used for communication between individual system components. Their choice in the case of communication between the controller and the SCADA system depends mainly on the choice of the controller manufacturer and the possibilities offered. Designers of non-dedicated SCADA systems most often provide a full range of connection options and data acquisition from the controller. Communication protocols such as Modbus or Profinet significantly facilitate the software of data transmission and reception; however, they do not provide sufficient security for such a connection in order to minimize the risk of a cyber-attack. By taking advantage of weaknesses, such as the lack of a properly complex authentication system, the lack of a unique key for communication or ensuring confidentiality and data integrity control, a hacker attack may damage or cause malfunction of the SCADA system.

The following are some examples of programs used to launch attacks: worms, viruses and Trojans:

Stuxnet

Stuxnet is a Windows-based computer worm that mainly targets devices using the Siemens WinCC SCADA system. It was detected in 2010 for the first time, and it is the first known worm used to spy on and make changes to the software of industrial installations. According to an independent Symantec report [87], Stuxnet is one of the most comprehensive cybersecurity threats facing industrial automation networks today. The Stuxnet worm mainly selects specific control systems related to services essential for the operation of the state (e.g., gas pipeline networks and power plants). The main purpose of this malware is to sabotage the production process by making changes in the PLC algorithms and hiding these changes from the SCADA system. Stuxnet has been used most widely in Iran, and despite its discovery in 2010, there are indications that the worm may have existed more than a year earlier and would have been undetected for that period of time. The complexity of the threat posed by Stuxnet has significantly influenced the perception of cybersecurity of industrial systems. Despite the fact that this worm mainly targets networks based on Siemens controllers, it is not difficult to imagine

its modifications aimed at infecting third-party controllers or other industrial automation equipment in general.

Industroyer

Industroyer is a malware of the framework, which is considered to be the main tool used during the attack on a Ukrainian power plant in 2016. As a result of this attack, approximately one million people were deprived of electricity for six hours. Industroyer is the first known software designed specifically to attack power plant networks. The analysis of this malware allows conclusions to be drawn regarding the security of communication protocols compliant with the standards. It should be stressed, however, that it is the weaknesses of the outdated SCADA system that allow the use of this framework. This is because, in the first place, it is the control and data acquisition system that allows unsecured access to freely manipulate the process data along with all the information about the devices connected in the industrial network.

Havex

Havex is a Trojan-type malware whose main purpose is to steal information about the production process and transfer it to the server acting as the remote access point of the attacker [88]. It was discovered in 2013 as part of an anti-spyware campaign. Its reach probably included thousands of industrial infrastructure facilities, especially in Europe and the United States. Once installed, Havex scanned the industrial network for any supervisory control and data collection (SCADA) devices. Then, using the OPC standard (OLE for Process Control), which is a universal communication protocol in industry, it sent to the command server data such as the program identifier, OPC standard version, information about the supplier, operation status as well as bandwidth and the name of the SCADA server. Havex was a tool designed to gather intelligence about the state of the production process and its technical details. It was used only for espionage, but the data obtained with it were probably intended to develop potential attacks on specific targets or entire industries.

3.3.2. Cloud SCADA Systems

SCADA systems in the cloud are an increasingly popular option when implementing new solutions in the industry. They can offer a reliable and secure approach to control, and resources and employees can be supplemented by remote support, continuous monitoring and automatic updates that are provided by the service. Design of communication between the systems is similar to the solutions in earlier SCADA systems; however, the matter is different if the cybersecurity of such systems is concerned. The problem of cybersecurity is crucial when approaching any of the implementations as the number of threats to industrial control systems is constantly increasing. In SCADA systems based on cloud operations, cybersecurity measures are very often ignored or applied inappropriately to the problem. Unsecured connections via satellite, radio communication or even network infrastructure give hackers the opportunity to target even distant objects.

3.3.3. HMI

Human–Machine Interface (HMI) is an industrial interface between a machine or process and the operator. By using the HMI, it is possible to influence the course of the process and its control in a more friendly environment than the set of PLC registers. Modern operator panels can be remotely controlled. They are also equipped with software and touch screens, which greatly facilitates the exchange of information at the human-machine level. The task of the HMI is to provide the operator with up-to-date, real information in a form that allows to make the best decision at a given moment of machine operation. The SCADA system is more complex and has a more extensive visualization of the entire process compared to HMI panels. The HMI panel is usually used for communication with individual devices. The SCADA system collects data from all devices that have a significant impact on the process and visualizes this data in one place, creating a comprehensive collection of all available information about the process.

The most important threats considered in the context of HMI is authorization management. Often, different levels of access are created on the machines, depending on the operator's rights, in order to protect against unauthorized changes to the parameters of the production process. According to the SANS report, in 89% of cases, such separation takes place using a different level of passwords [86]. However, providers of equipment and the environment that allows the creation of HMIs most often save passwords in the memory registers of operator panels, which are not secured by any encryption method or simply force the storage of passwords in the memory of the PLC controller, and thus handling the authorization request from its level. Assuming that the operator panel communicates with the PLC using one of the known communication standards (e.g., Ethernet), it is not difficult to imagine a way to carry out an attack using the data obtained through the MIM listening device. In addition, it is worth considering the case in which SCADA has full access to the operator panel registers in accordance with the priority of its control, which may lead to distributed hacking attacks on the level of the entire industrial network system.

Another source of problems related to HMIs is the lack of an encrypted connection with the controllers, which is most often based on data transmission protocols used according to industrial standards. This is because software producers strive to standardize the services offered in order to ensure compatibility with as many devices and external programs as possible. The use of this type of unsecured connection allows to carry out successful MIM attacks and simulate the operation of any of the elements by transmitting a previously modified intercepted communication frame.

According to the report prepared by TrendMicro [89], as much as 20% of the identified threats from HMI refer to the lack of security in the operator panels' memory and software. Often the way the memory is built in the operator panels forces the integrators team to implement the simplest memory management mechanisms, defined by the programming environment offered by the manufacturer. The main element to consider when designing HMI is the method of securing the code and security related to reading and writing data that go beyond the defined range.

3.3.4. Other Software in Computers and Servers

The amount of data processed and the level of advancement of applications necessary for the proper management of production in modern industrial plants can overwhelm even the most efficient computers. Therefore, industrial servers are used to handle tasks that require enormous computing power. Among the active elements in the network, we can also distinguish process computers, aimed to control the process parameters through dedicated applications (process interface) that support many different hardware environments. The issue of using PCs as elements of an industrial network is also important. The hardware of this type of equipment is of little importance from the point of view of cybersecurity. However, the greatest attention should be paid to the issue of operating systems and applications running on these systems. The most commonly used computer operating systems in industry are the Windows family and real-time systems. This is mainly caused by the requirements of SCADA, ERP or MES software producers. The popularity of Windows systems is, however, associated with the widespread information about their weaknesses and translates into the number of tools available to carry out hacker attacks.

Several important aspects related to the security of computers and servers in industrial networks are listed below:

Firewalls

The term inherent in the cybersecurity of industrial network software is a firewall. It acts as a combination of hardware and software protection of the internal network against external access (public networks and the Internet). Its task is also to protect against unauthorized outflow of data from the local network to the outside. The role of a firewall can be played by a specially designed device with appropriate software or the software itself located on access points equipped with a data packet management system. The most frequently used protection techniques in a firewall is packet filtering consisting in

checking their origin and managing the system of their acceptance, using algorithms for the purposes of user identification and securing programs that support certain data transmission protocols.

An important function of a firewall from the cybersecurity of industrial networks point of view is the network traffic monitoring and events logging. This enables authorized persons to make early changes to the firewall configuration and makes it much easier during the risk monitoring phase. The firewall also allows to define a zone of limited trust, and thus create a subnet that isolates local servers providing services from the internal network.

Industrial versions of firewalls can protect the industrial network against unauthorized access by filtering IP addresses, MAC addresses, ports dedicated to specific industrial protocols as well as monitor the correctness of the frame structure of a given protocol. However, they will not protect against data modification in a properly built frame, when it is secured only with a checksum with a well-known algorithm.

Up-to-Date Software

According to the CyberX report, as many as 53% of manufacturing companies still use Windows XP [70]. Lack of support for Windows XP as well as other outdated operating systems means a significant risk of hacking attacks due to the lack of further patches to prevent this type of activity. Analyzing the source code of the malware Stuxnet, it was noticed that it mainly exploited the flaws of the Windows system in order to reproduce itself on other devices.

However, the problem of keeping operating systems up-to-date on PCs is complex because it depends mainly on the compatibility of the software provided by the manufacturer of the process automation equipment (allowing the creation/modification of the program). In order to update the operating system, it is necessary to verify whether the program under the given license can run on the new version of the system.

The problem of up-to-date software related to servers concerns mainly the classic construction of an industrial control network, based on a server located inside the plant (in the local communication network). Cloud-based information-processing systems usually offer the latest technological solutions related to the software of their web servers. Nevertheless, outdated software of industrial servers affects the cybersecurity of internal networks in a similar way as the up-to-date software of PCs operating with the use of this network. A significant amount of malware is contained in devkit for network systems based on old Windows Server systems.

Anti-Virus Software

The basic tool for protection against malware on PCs is antivirus software. The vast majority of successfully carried out hacking attacks related to industrial networks began by infecting a PC resulting from opening an infected attachment in an e-mail or visiting a properly prepared website [72]. Despite this, as many as 57% of production units do not have anti-virus software in their security system [70]. Additionally, as the CyberX report shows, as many as 67% of companies with antivirus software have exclusive automatic updates of the malware database.

Due to the dynamic cooperation of software producers with the management and reporting units on potentially dangerous situations established under the NIS Directive, fear of being up-to-date with the list of threats has become a much simpler task and one of the most important elements of cybersecurity.

Flame

Flame is a complex malware discovered in 2012 by Kaspersky Lab [90]. It is characterized by a combination of several elements to be classified in the group of Trojan viruses, viruses bypassing authorization and computer worms. Source code analysis of this malware revealed links to the Stuxnet virus. As with Stuxnet, this malware was discovered in the Middle East and this region was the main target of the attacks. The principle of operation of this malware turned out to be a collision attack, which consisted of generating two different strings of characters, which after processing give the same checksum on

the output. Thanks to this, Flame was able to forge and use Microsoft Windows Update certificates to sign its code. The analysis of this malware showed that it ran for 5 years and the complete source code consisted of almost 20 different modules and took up 20 MB. Unlike Stuxnet, Flame was only used for comprehensive data stealing from business units in the Middle East.

Duqu

Duqu is a backdoor [91] malware whose main purpose is to collect information from the infected Windows operating system and forward it to the server managing the attack. It was discovered in 2011, and its source code indicates a close link to the Stuxnet worm. The main targets of the attack were, as in the case of Stuxnet and Flame, the countries of the Middle East. Duqu did not attack SCADA systems and PLCs as was the case of Stuxnet worm. However, this tool was designed only to launch a hacker attack targeting industrial systems, and its purpose was not to sabotage but to steal data from computers. Duqu collected data in the form of screenshots and sent it in encrypted transmission to a remote server. An interesting aspect of the operation is the fact that it is not detectable by antiviruses because Duqu was attacking through ring0; so, at the level of the operating system kernel (to which antivirus software simply cannot access). The first infection probably took place as a result of opening an infected email attachment. Duqu is only set to run for 36 days and then automatically removes itself from the system.

4. Where Most Urgent Actions Are Required in Industrial Control Network Systems?

4.1. Higher Security Standards in Communication Protocols

From the point of view of industrial networks, the weakest point is industrial communication protocols. This is mainly due to the security of the entire network infrastructure was not taken into account when creating the standards. Thus, the use of solutions based on the industrial Ethernet protocol does not always ensure data integrity, confidentiality and authentication. By exploiting the weaknesses of communication protocols, an attacker can carry out many successful attacks using techniques such as Man in the Middle or forcing outputs with simulating a SCADA response. During the analysis of the majority of the risks it is industrial data transmission methods were the most vulnerable point. Despite the facilitation, which is undoubtedly the use of standard communication protocols, people involved in the creation of machines should pay particular attention to the chosen methods of data transmission between subsequent elements in the industrial network. This is mainly because retrofitting to reduce the risk can simply be too costly.

One way to "strengthen" the security of industrial protocols is to transmit some redundant data that are checksums for the actual data. The algorithm for calculating the checksum could be embedded in the form of a permanent code on the side of the devices involved in the communication for the purpose of encoding, decoding and verifying the data. The resulting data packet would be difficult to interpret and replace, and the use of random values would not be accepted by the receiving device because the control criterion was not met.

4.2. Improvements in the Industrial Network Architecture

The second place that influences the risk of a successful hacker attack in industrial network systems is the network topology. When analyzing the operation of computer worms such as LogicLocker or Stuxnet, it is possible to clearly determine which weaknesses of the industrial network topology were used to carry out an effective attack. In addition, as reports related to the cybersecurity of industrial networks indicate, there is no concept of complete separation of industrial elements from the global network. According to a report by CyberX [80], as many as 40% of industrial units have at least one direct connection to the global network. Trends, on the other hand, show that the number of machine connections to the network is constantly increasing, and this is closely related to the idea of Industry 4.0, which mainly assumes the integration of IT and OT in industry.

During the analysis of the Stuxnet worm, it was indicated that the network topology was used for cloning. The principle of LogicLocker's operation was the ability to move horizontally or vertically to the attacked PLC. It is also worth noting that cloud-distributed SCADA systems, which by definition require full integration of industrial control equipment with the network, are becoming more and more popular. Adequate protection of data transmission protocols usually belongs to the manufacturer offering the technological solution; however, there remains the issue of proper care for the security of the network topology and the connected devices.

4.2.1. Division of the Industrial Network into Subnetworks

The first proposed solution related to the network topology is conscious and intelligent division of the industrial network into subnets while isolating the control elements in the production process. This is particularly important from the cybersecurity point of view due to the physical limitation of access to the attack-sensitive elements in the internal network. The proposed solution is largely based on the statistical data presented in the analyzed reports during the study of places that affect the risk of a hacker attack. The key to effective network division is the mapping of active devices and the creation of an information flow diagram in a given network. On the basis of the obtained data, it is possible to determine the parameters necessary for the correct configuration of the firewall. For example, for systems of self-monitoring of the process, it is possible to block sending feedback to the actuators.

The effective division of the industrial network is an important element for cybersecurity due to the isolation of the production process from network access points not related in any way to supervision or data acquisition from this process. This reduces the risk that human error. At the same time, the production process, in order to ensure the maximum level of safety, should be separated from the industrial network by means of the so-called air barrier. This term refers to avoiding the connection of all controllers in the network, but only those which are necessary for the proper supervision of the production process while using the child connection of the rest of the controllers in the production line (using other methods of data transmission between them). Such action reduces the visibility of the full process in a hacker attack and protects part of the production line against the negative effects of such an attack.

For external connections to an internal industrial network, it is possible to use encrypted connection using VPN. The main purpose of VPN is to ensure the exchange of data between the external device and the internal network of the enterprise in such a way that the nodes of this network remain invisible to the data packets transmitted in this way. Thanks to the use of VPN, it is also possible to compress and encrypt the transmitted data in order to ensure a higher level of security. It requires, however, correct configuration of the service, performed according to the network topology and transmission protocols used in it. Such a solution is also aimed at securing the access point to the network and the element implementing the connection by hiding the transmission parameters from the level of the global Internet network.

If remote access is necessary one of the safe solutions is the production server copy using OPC technology, as proposed in Figure 4, with Siemens solutions. In this solution, WebNavigator and/or DataMonitor Clients [92], accessed via a web browser, can be used to control and monitor some aspects of the process. VPN and Firewall solutions applied as described above also should be used to minimize and monitor the risks.

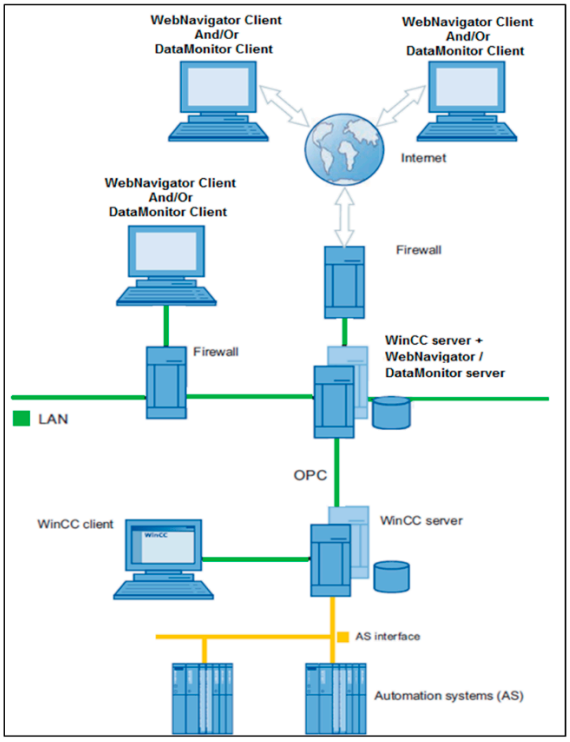

Figure 4. Exemplary structure of the network with Siemens solutions for remote access.

4.2.2. Integrity Checking

The second way to reduce the risks arising from the network topology is to skillfully use the transmitted data integrity checking. The proposed solution and its application to the active elements were used to build the network. One way to control data integrity is to transfer data in two ways with a later data comparison. The method involves using two communication ports to send the same message with the verification of the compliance of both messages on the final active element of the network that can perform this verification. Such protection significantly excludes the possibility of distorting the transmitted data during the communication process, thus limiting the possibility of a hacker attack consisting of changing the data frame. The assumption of such a method of data control is mainly based on an appropriate device capable of comparing the communication frame on two ports, and thus is not fully universal. On the other hand, the verification can thus be carried out, e.g., directly in the PLC controller into which the data (commands) are transferred. However, this requires a greater effort on the part of the programmer.

Another way is to introduce multi-stage operation confirmation. The assumption of this method is to execute a command from the level of a remote SCADA system requiring confirmation from the machine operator by confirming the received and displayed parameters on the HMI panel before rewriting them to the controller registers. Such a solution, despite the simplicity of implementation, may negatively affect the time of entering settings. For this reason, in order to implement this solution, close cooperation between the machine operator and the SCADA system operator is necessary.

The last proposed way to maintain data integrity in the context of the entire industrial network is to automate the process of creating copies of data. The issue of creating automatic backups is particularly difficult with older driver models. Therefore, a holistic approach is necessary, which—before the command is executed by the controller—allows to download a set of register values and compares them with previously saved values. This method of data storage may significantly affect the integrity of the data due to the possibility of quick restoring the complete information to the registers taken over as a result of a hacking attack. Such a solution works especially in systems where few values or parameters of the process are changed, as it requires the creation of additional data areas.

4.2.3. Monitoring of the Data Transmission Authorization

Monitoring the authorization of transmitted data is also one of the most important concepts in the field of industrial networks cybersecurity. The presented solution aims to limit unauthorized changes to data by introducing a system of authorizations and a cascade system of data correctness confirmation. Effective and continuous monitoring of authorization requires the creation of a central server that supports the operation of network user verification, encryption and receiving encrypted connections. Connection to the global network should be made only through the aforementioned server, which, based on the provided login data, would use the pool of available sites for each group of users.

The main purpose of introducing a central authorization system is to secure communication between two access points that are elements of the process data exchange. This is especially important in the case of data exchange between two SCADA systems that supervise equivalent processes and require connection via the global network. In this case, it is possible to create a header containing the authorization data of each of the systems and then encrypt these data passing through the authorization server in question. Efficient encryption of data based on a key and their authorization can be performed in many ways using algorithms such as DES or SHA-3.

The cascade data validation system assumes verification both through a central authorization system and a properly configured firewall. Such action is aimed to prevent unwanted modification of transmitted data already within the industrial network. However, it should be remembered that user authorization systems usually cannot be used in the case of older control systems and most independent measurement devices, due to the lack of support from the central data authorization mechanism.

The advantage of introducing an authorization system is the ability to monitor network activity and encrypt connections between access points in a given network. Logs from such a system can be a good starting point when analyzing security during an audit. Additionally, the creation of a central authorization server enables blocking of unwanted connections with remote-control servers during attacks due to the lack of a unique key.

4.3. Control and Updating of the Software

The problem of software validity control seems to be particularly important due to the growing awareness of device manufacturers and anti-virus application vendors. Since the detection of the Stuxnet worm, the databases of malware in anti-virus applications targeting industrial devices have grown steadily. Companies such as Symantec or Kaspersky LAB have established special units to identify and eliminate potential threats related to cybersecurity of industrial networks. In addition, updates of subsequent versions of the tools for programming controllers introduce new solutions aimed at reducing the risk. Examples of worms such as Flame or Duqu also prove that it is equally important to keep the operating system up-to-date on computers in the industrial network. Malicious software used counterfeit Windows certificates or special system toolkits. Subsequent updates of the operating system eliminated the exploited vulnerabilities. Therefore, it is extremely important to have an up-to-date malware database in order to correctly and quickly detect a threat. In the case of extensive industrial networks, however, this can be quite a challenge for cybersecurity staff.

The proposed method of checking for up-to-date software simplifies and automates this process by creating automatic scripts that allow to check the application version. The scripts, along with the periodic execution command, should be implemented on each computer in the internal industrial network. The obtained information should be sent to the network administrator, aimed at performing the required updates. Automating the process of collecting information about installed software versions can significantly facilitate the work of determining which applications require updating, but the software update should be carried out by persons with appropriate permissions. Improper execution of this process (e.g., using infected software) may lead to an infection of the network (as was the case with the spread of the Havex virus).

4.4. Reduction of the Human Component

Most of the examples of successful (malicious) hacking attacks discussed here arose due to human error. The most common initiation of an attack is opening an infected attachment in an e-mail or downloading files from websites with a forged certificate. Despite the fact that people's awareness of cybersecurity is growing every year, the human factor is still the main source of risk. Even the best-configured firewalls will not provide adequate protection for a user who does not maintain basic computer hygiene related to network resources. Many companies have a special policy related to access to the global network from devices in the internal industrial network, but most often it comes down to a pool of blocked sites, ports or services. Raising staff awareness of cybersecurity thus remains one of the most important elements requiring the most urgent action.

The most effective method of raising staff awareness is organizing periodic training. For new and unfamiliar users of the industrial network, it is a great way to learn about the rules of the plant and learn the basic rules of hygiene in the network. Based on the completed training and control tests, it is possible to define the permissions for a given user (depending on his level of understanding of these issues).

The number of threats is constantly increasing, and therefore new security methods and special rules are introduced to limit the possibility of infecting the local network. Therefore, it is necessary to periodically organize supplementary and qualification-raising trainings.

5. Conclusions

The Industry 4.0 concept in its core assumptions takes good advantage of new, arising technologies. It also aims to introduce in the manufacturing process some other technologies, well established in everyday life. Even if the stability, reliability and robustness issues of such technologies are reaching industry standards, the cybersecurity of the new solutions poses the greatest challenge of all. In some cases, it may be the main obstacle in the transition to Industry 4.0 and usage of all its benefits. As described in this article, the key issue is the proper analysis of the system vulnerabilities, knowledge about the external and internal threats, responsible design of the system architecture and a dedicated risk management plan. While this article was not intended to analyze and compare different methods of risk assessment and mitigation, exemplary solutions discussed in the article can indicate the way towards real transformation according to the fourth industrial revolution standards. Even if the technological aspects of cybersecurity will be well adopted, raising awareness and constant training among the employees at every corporate level can be of key importance. Only if the above actions are well performed the true potential of the Industry 4.0 idea can be achieved in a production entity.

Author Contributions: Conceptualization, J.H. and S.O.; literature review, S.O.; investigation, J.H.; writing—original draft preparation, J.H. and S.O.; writing—review and editing, R.J.; visualization, J.H. and R.J.; supervision, S.O. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was financed from the research subsidy at the Silesian University of Technology.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hofmann, E.; Rüsch, M. Industry 4.0 and the current status as well as future prospects on logistics. *Comput. Ind.* **2017**, *89*, 23–34. [CrossRef]
2. Rojko, A. Industry 4.0 Concept: Background and Overview. *Int. J. Interact. Mob. Technol.* **2017**, *11*, 77–90. [CrossRef]
3. Wagner, T.A.; Herrmann, C.; Thiede, S. Industry 4.0 Impacts on Lean Production Systems. *Procedia CIRP* **2017**, *63*, 125–131. [CrossRef]

4. Lu, Y. Industry 4.0: A survey on technologies, applications and open research issues. *J. Ind. Inf. Integr.* **2017**, *6*, 1–10. [CrossRef]
5. Grieco, A.; Caricato, P.; Gianfreda, D.; Pesce, M.; Rigon, V.; Tregnaghi, L.; Voglino, A. An Industry 4.0 Case Study in Fashion Manufacturing. *Procedia Manuf.* **2017**, *11*, 871–877. [CrossRef]
6. Motyl, B.; Baronio, G.; Uberti, S.; Speranza, D.; Filippi, S. How will Change the Future Engineers' Skills in the Industry 4.0 Framework? A Questionnaire Survey. *Procedia Manuf.* **2017**, *11*, 1501–1509. [CrossRef]
7. Weyer, S.; Schmitt, M.; Ohmer, M.; Gorecky, D. Towards Industry 4.0—Standardization as the crucial challenge for highly modular, multi-vendor production systems. *IFAC-Papersonline* **2015**, *48*, 579–584. [CrossRef]
8. Micklethwait, J.; Wooldridge, A. *The Global Race to Reinvent the State*; Penguin Press: London, UK, 2015.
9. Berger, R. *The Industrie 4.0 Transition Quantified. How the Fourth Industrial Revolution Is Reshuffling the Economic, Social and Industrial Model*; Roland Berger: Monachium, Germany, 2016.
10. Sader, S.; Husti, I.; Daróczi, M. Industry 4.0 as a Key Enabler toward Successful Implementation of Total Quality Management Practices. *Period. Polytech. Soc. Manag. Sci.* **2019**, *27*, 131–140. [CrossRef]
11. Cimini, C.; Boffelli, A.; Lagorio, A.; Kalchschmidt, M.; Pinto, R. How do industry 4.0 technologies influence organisational change? An empirical analysis of Italian SMEs. *J. Manuf. Technol. Manag.* **2020**, *32*, 695–721. [CrossRef]
12. Pereira, A.G.; Lima, T.; Charrua-Santos, F. Industry 4.0 and Society 5.0: Opportunities and Threats. *Int. J. Recent Technol. Eng.* **2020**, *8*, 3305–3308. [CrossRef]
13. Zengin, Y.; Naktiyok, S.; Kaygın, E.; Kavak, O.; Topçuoğlu, E. An Investigation upon Industry 4.0 and Society 5.0 within the Context of Sustainable Development Goals. *Sustainability* **2021**, *13*, 2682. [CrossRef]
14. Pereira, A.G.; Lima, T.M.; Charrua-Santos, F. Society 5.0 as a Result of the Technological Evolution: Historical Approach. *Adv. Intell. Syst. Comput.* **2020**, *1018*, 700–705. [CrossRef]
15. Peruzzini, M.; Grandi, F.; Pellicciari, M. Benchmarking of Tools for User Experience Analysis in Industry 4.0. *Procedia Manuf.* **2017**, *11*, 806–813. [CrossRef]
16. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–4.
17. Rossit, D.A.; Tohmé, F.; Frutos, M. Production planning and scheduling in Cyber-Physical Production Systems: A review. *Int. J. Comput. Integr. Manuf.* **2019**, *32*, 385–395. [CrossRef]
18. Lee, J.; Bagheri, B.; Kao, H.-A. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
19. Baena, F.; Guarin, A.; Mora, J.; Sauza, J.; Retat, S. Learning Factory: The Path to Industry 4.0. *Procedia Manuf.* **2017**, *9*, 73–80. [CrossRef]
20. Leyh, C.; Martin, S.; Schäffer, T. Industry 4.0 and Lean Production—A Matching Relationship? An analysis of selected Industry 4.0 models. In Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, Prague, Czech Republic, 3–6 September 2017; Volume 11, pp. 989–993.
21. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
22. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
23. Da Xu, L.; He, W.; Li, S. Internet of Things in Industries: A Survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]
24. Industrial Internet of Things, A Quarterly Supplement of Automation World, August 2021. Available online: https://s3.amazonaws.com/public-files.cloud.pmmimediagroup.com/campaigns/34829/ads/86154/2108_IIOT_EBook_V2.pdf (accessed on 23 September 2021).
25. Lee, I. The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet Things* **2019**, *7*, 100078. [CrossRef]
26. Malik, V.; Singh, S. Security risk management in IoT environment. *J. Discret. Math. Sci. Cryptogr.* **2019**, *22*, 697–709. [CrossRef]
27. Balaji, V.; Venkumar, P.; Sabitha, M.S.; Amuthaguka, D. DVSMS: Dynamic value stream mapping solution by applying IIoT. *Sadhana* **2020**, *45*, 1–13. [CrossRef]
28. ETSI. Cyber Security for Consumer Internet of Things. 2019. Available online: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (accessed on 24 September 2021).
29. Moreno-Vozmediano, R.; Montero, R.; Llorente, I.M. Key Challenges in Cloud Computing: Enabling the Future Internet of Services. *IEEE Internet Comput.* **2012**, *17*, 18–25. [CrossRef]
30. Cardoso, J.; Barros, A.; May, N.; Kylau, U. Towards a Unified Service Description Language for the Internet of Services: Requirements and First Developments. In Proceedings of the 2010 IEEE International Conference on Services Computing, Miami, FL, USA, 5–10 July 2010; pp. 602–609.
31. Gandomi, A.; Haider, M. Beyond the hype: Big data concepts, methods, and analytics. *Int. J. Inf. Manag.* **2015**, *35*, 137–144. [CrossRef]
32. Chen, M.; Mao, S.; Liu, Y. Big Data: A Survey. *Mob. Netw. Appl.* **2014**, *19*, 171–209. [CrossRef]
33. Peters, E.; Klieštik, T.; Musa, H.; Durana, P. Product Decision-Making Information Systems, Real-Time Big Data Analytics, and Deep Learning-enabled Smart Process Planning in Sustainable Industry 4.0. *J. Self-Gov. Manag. Econ.* **2020**, *8*, 16–22.

34. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge Computing: Vision and Challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646. [CrossRef]
35. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 17 August 2012; pp. 13–16.
36. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; et al. A view of cloud computing. *Commun. ACM* **2010**, *53*, 50–58. [CrossRef]
37. Muniswamaiah, M.; Agerwala, T.; Tappert, C.C. Fog Computing and the Internet of Things (IoT): A Review. In Proceedings of the 2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Washington, DC, USA, 26–28 June 2021; pp. 10–12.
38. Etawi, A. A comparison between cluster, grid, and cloud computing. *Int. J. Comput. Appl.* **2018**, *179*, 37–42.
39. Ghorbel, A.; Ghorbel, M.; Jmaiel, M. Privacy in cloud computing environments: A survey and research challenges. *J. Supercomput.* **2017**, *73*, 2763–2800. [CrossRef]
40. Senyo, P.K.; Addae, E.; Boateng, R. Cloud computing research: A review of research themes, frameworks, methods and future research directions. *Int. J. Inf. Manag.* **2018**, *38*, 128–139. [CrossRef]
41. Varghese, B.; Buyya, R. Next generation cloud computing: New trends and research directions. *Future Gener. Comput. Syst.* **2018**, *79*, 849–861. [CrossRef]
42. Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Comput. Secur.* **2018**, *74*, 340–354. [CrossRef]
43. Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, A.V. Security and Privacy for Cloud-Based IoT: Challenges. *IEEE Commun. Mag.* **2017**, *55*, 26–33. [CrossRef]
44. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. *IOT* **2018**, *1*, 1–13. [CrossRef]
45. Rao, A.R.; Clarke, D. Perspectives on emerging directions in using IoT devices in blockchain applications. *Internet Things* **2020**, *10*, 100079. [CrossRef]
46. Narayanaswamy, T.; Karthika, P.; Balasubramanian, K. Blockchain Enterprise: Use Cases on Multiple Industries. In *EAI/Springer Innovations in Communication and Computing*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 125–137.
47. Lim, M.K.; Li, Y.; Wang, C.; Tseng, M.-L. A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. *Comput. Ind. Eng.* **2021**, *154*, 107133. [CrossRef]
48. Upadhyay, A.; Ayodele, J.O.; Kumar, A.; Garza-Reyes, J.A. A review of challenges and opportunities of blockchain adoption for operational excellence in the UK automotive industry. *J. Glob. Oper. Strat. Sourc.* **2021**, *14*, 7–60. [CrossRef]
49. Rea-Guaman, A.M.; Mejía, J.; Feliu, T.S.; Calvo-Manzano, J.A. Avarciber: A framework for assessing cybersecurity risks. *Clust. Comput.* **2020**, *23*, 1827–1843. [CrossRef]
50. Mullet, V.; Sondi, P.; Ramat, E. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access* **2021**, *9*, 23235–23263. [CrossRef]
51. Peshkin, M.A.; Colgate, J.E.; Wannasuphoprasit, W.; Moore, C.A.; Gillespie, R.B.; Akella, P. Cobot architecture. *IEEE Trans. Robot. Autom.* **2001**, *17*, 377–390. [CrossRef]
52. El Zaatari, S.; Marei, M.; Li, W.; Usman, Z. Cobot programming for collaborative industrial tasks: An overview. *Robot. Auton. Syst.* **2019**, *116*, 162–180. [CrossRef]
53. Malik, A.A.; Bilberg, A. Complexity-based task allocation in human-robot collaborative assembly. *Ind. Robot. Int. J.* **2019**, *46*, 471–480. [CrossRef]
54. Fernández-Caramés, T.M.; Fraga-Lamas, P. Use Case Based Blended Teaching of IIoT Cybersecurity in the Industry 4.0 Era. *Appl. Sci.* **2020**, *10*, 5607. [CrossRef]
55. Thames, L.; Schaefer, D. Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges. In *Hybrid Manufacturing Processes*; Springer: Cham, Switzerland, 2017; pp. 1–33.
56. Ogonowski, S.; Ogonowski, Z.; Pawełczyk, M. Multi-Objective and Multi-Rate Control of the Grinding and Classification Circuit with Electromagnetic Mill. *Appl. Sci.* **2018**, *8*, 506. [CrossRef]
57. Langmann, R.; Rojas-Pena, L.F. A PLC as an Industry 4.0 component. In Proceedings of the 2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV), Madrid, Spain, 24–26 February 2016; pp. 10–15.
58. Langmann, R.; Stiller, M. The PLC as a Smart Service in Industry 4.0 Production Systems. *Appl. Sci.* **2019**, *9*, 3815. [CrossRef]
59. Yamada, T.; Nakano, T.; Kaji, T.; Tano, S. Security Introduction Framework for Operational Technologies and Applying to Industrial Control System. In Proceedings of the 2020 59th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), Chiang Mai, Thailand, 23–26 September 2020; pp. 25–30.
60. Wagner, P.; Hansch, G.; Konrad, C.; John, K.-H.; Bauer, J.; Franke, J. Applicability of Security Standards for Operational Technology by SMEs and Large Enterprises. In Proceedings of the 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 8–11 September 2020; Volume 1, pp. 1544–1551.
61. Alshaikh, M.; Maynard, S.; Ahmad, A.; Chang, S. An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. In Proceedings of the 50th Hawaii International Conference on System Sciences (2017), Waikoloa Village, HI, USA, 1 March–1 June 2018.
62. Gundu, T. Acknowledging and Reducing the Knowing and Doing gap in Employee Cybersecurity Compliance. In Proceedings of the International Conference on Cyber Warfare and Security, Stellenbosch, South Africa, 28 February–1 March 2019; pp. 94–102.

63. Silic, M.; Lowry, P.B. Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. *J. Manag. Inf. Syst.* **2020**, *37*, 129–161. [CrossRef]
64. Krumay, B.; Bernroider, E.W.N.; Walser, R. Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. *Lecture Notes Comput. Sci.* **2018**, *11252*, 369–384.
65. European Union. General Data Protection Regulation GDPR. Available online: https://gdpr-info.eu (accessed on 23 September 2021).
66. Jayakrishnan, G.C.; Sirigireddy, G.R.; Vaddepalli, S.; Banahatti, V.; Lodha, S.P.; Pandit, S.S. Passworld: A serious game to promote password awareness and diversity in an enterprise. In Proceedings of the 16th Symposium on Usable Privacy and Se-curity, Boston, MA, USA, 10–11 August 2020; pp. 1–18.
67. Kuypers, M.; Maillart, T. Designing Organizations for Cyber Security Resilience. In Proceedings of the 2018 the Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria, 18–19 June 2018.
68. Chen, Q.; Abercrombie, R.K.; Sheldon, F.T. Risk Assessment for Industrial Control Systems Quantifying Availability Using Mean Failure Cost (MFC). *J. Artif. Intell. Soft Comput. Res.* **2015**, *5*, 205–220. [CrossRef]
69. Stouffer, K.; Falco, J.; Scarfone, K. *Guide to Industrial Control Systems (ICS) Security*; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2011.
70. CyberX Labs. 2019 Global ICS & IIoT Risk Report. 2019. Available online: https://cdn2.hubspot.net/hubfs/2479124/CyberX%20Global%20ICS%20%2F%20IIoT%20Risk%20Report.pdf (accessed on 5 September 2021).
71. Joinson, A.; van Steen, T. Human aspects of cyber security: Behaviour or culture change? *Cyber Secur. Peer-Rev. J.* **2018**, *1*, 351–360.
72. Verizon 2020 Data Breach Investigations Report. Available online: https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf (accessed on 5 September 2021).
73. Cj, G.; Pandit, S.; Vaddepalli, S.; Tupsamudre, H.; Banahatti, V.; Lodha, S. PHISHY—A Serious Game to Train Enterprise Users on Phishing Awareness. In Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts, Melbourne, Australia, 28–31 October 2018; pp. 169–181.
74. Takata, T.; Ogura, K. Confront Phishing Attacks—From a Perspective of Security Education. In Proceedings of the 2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST), Morioka, Japan, 23–25 October 2019; pp. 10–13.
75. Reinheimer, B.; Aldag, L.; Mayer, P.; Mossano, M.; Duezguen, R. An investigation of phishing awareness and education over time: When and how to best remind users. In Proceedings of the Sixteenth Symposium on Usable Privacy and Security, Michigan, MN, USA, 10–11 August 2020; pp. 259–284.
76. Liberati, F.; Garone, E.; Di Giorgio, A. Review of Cyber-Physical Attacks in Smart Grids: A System-Theoretic Perspective. *Electronics* **2021**, *10*, 1153. [CrossRef]
77. Su, Q.; Wang, H.; Sun, C.; Li, B.; Li, J. Cyber-attacks against cyber-physical power systems security: State estimation, attacks reconstruction and defense strategy. *Appl. Math. Comput.* **2022**, *413*, 126639. [CrossRef]
78. Wang, P.-B.; Ren, X.-M.; Zheng, D.-D. Event-triggered resilient control for cyber-physical systems under periodic DoS jamming attacks. *Inf. Sci.* **2021**, *577*, 541–556. [CrossRef]
79. Tan, J.; Bauer, L.; Christin, N.; Cranor, L.F. Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-strength, Minimum-length, and Blocklist Requirements. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual, Korea, 15–19 November 2020.
80. Huynh, D.; Luong, P.; Iida, H.; Beuran, R. Design and Evaluation of a Cybersecurity Awareness Training Game. In *Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2017; Volume 10507, pp. 183–188.
81. Sunshine Coast Daily. Available online: https://www.sunshinecoastdaily.com.au/news/some-of-our-history-of-hacking-is-known-the-world-/3126317 (accessed on 20 June 2020).
82. SecurityFocus. Available online: https://www.securityfocus.com/news/6767 (accessed on 18 June 2020).
83. Johnson, R.E. Survey of SCADA security challenges and potential attack vectors. In Proceedings of the International Conference for Internet Technology and Secured Transactions, London, UK, 8–10 December 2010.
84. Beyah, R.; Formby, D.; Durbha, S. Out of Control: Ransomware for Industrial Control Systems. Available online: https://pdfs.semanticscholar.org/5add/591abd9b773c8176df41fceb920a485eff79.pdf (accessed on 1 September 2021).
85. Schwartke, H.; Spenneberg, R.; Brüggemann, M. PLC-Blaster: A Worm Living Solely in the PLC. Available online: https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf (accessed on 8 September 2021).
86. SANS 2019 State of OT/ICS Cybersecurity Survey. Available online: https://www.forescout.com/resources/2019-sans-state-of-ot-ics-cybersecurity-survey (accessed on 5 September 2021).
87. Murchu, L.O.; Falliere, N.; Chien, E. W32.Stuxnet Dossier. 2010 Symantec Security Response. Available online: https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf (accessed on 8 September 2021).
88. F-Secure. Threat Description Backdoor: W32/Havex. Available online: https://www.f-secure.com/v-descs/backdoor_w32_havex.shtml (accessed on 8 September 2021).
89. TrendMicro. The State of SCADA HMI Vulnerabilities. Available online: https://www.trendmicro.com/vinfo/pl/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities (accessed on 5 September 2021).

90. SecureList. The Flame: Questions and Answers. Available online: https://securelist.com/the-flame-questions-and-answers/34344 (accessed on 8 September 2021).
91. F-Secure. Threat Description Backdoor: W32/Duqu. Available online: https://www.f-secure.com/v-descs/backdoor_w32_duqu.shtml (accessed on 8 September 2021).
92. SIMATIC HMI WinCC Basic Options, System Manual. Available online: https://cache.industry.siemens.com/dl/files/233/109736233/att_879853/v1/WinCC_BasicOptions_en-US_en-US.pdf (accessed on 28 September 2021).