Instituto Politécnico
de Viana do Castelo

Assessing Cybersecurity At An Industrial Unit 4.0

Silvino Pires Dos Santos

Escola Superior de Tecnologia e Gestão

Instituto Politécnico
de Viana do Castelo

Nome completo do candidato(a)

Silvino Pires Dos Santos

Nome do curso de Mestrado

Mestrado em Cibersegurança

Trabalho efetuado sob a supervisão de

Professor Paulo Jorge Campos Costa

Mestrado em Cibersegurança
Master in Cybersecurity

ASSESSING CYBERSECURITY AT AN INDUSTRIAL UNIT 4.0

a master's thesis authored by

Silvino Pires Dos Santos

and supervised by

Paulo Jorge Campos Costa
Professor Adjunto, IPVC

This thesis was submitted in partial fulfilment of the requirements for the Master's degree in Cybersecurity at the Instituto Politécnico de Viana do Castelo

17 of June, 2023

Abstract

The last 20 years have emerged significant developments in industrial production and development, with new technologies, networks and emerging production systems due to the development of the internet and new distributed adaptive production systems. These architectures resulted in improved service activities, new business models and increased demand and offering of goods, resulting in fewer interactions among production system participants.

The convergence of IT/OT environments has increased the complexity and vulnerability of previously isolated OT/ICS networks, and the growing need to expand automation in the industry creates a big challenge in terms of cybersecurity. In this context, how can we identify suspicious activity, assess risks and help prevent downtime in an increasingly technological industry?

For this thesis, data collected through an online survey on the subject of convergence in the national industry was analyzed in order to know if this subject, from the perspective of professionals, deserves the attention of the organizations where they develop their professional activity with technologies of IT/OT. A set of real cases and the consequences of serious security failures that occurred in the period between 2021 and 2023, increasingly common, with an impact on the global industry, are identified and analyzed.

The technological complexity that results from the convergence between information technology (IT) and Operational Technology (OT) is analyzed, highlighting in practice the challenges for which cybersecurity has to prepare itself in order to develop effective and context-adjusted responses under review. The biggest challenge lies in the cyber-secure integration of data-centric computing technologies in the IT systems with the monitoring of events, processes and devices in the OT systems.

After analyzing the complexity of the IT/OT technologies essential for Industry 4.0, we recommend a careful reading of the set of frameworks described in this document about internationally recognized good practices in cybersecurity. Regular access to public databases, described in this document, on risk patterns and fundamental vulnerabilities is recommended for the development of an updated cybersecurity strategy. Finally, good practices are described to analyze, frame and apply to avoid risk situations by monitoring the trend of cybersecurity incidents, known software flaws, as well as vulnerabilities and associated risks, which can result in ransomware and its associated consequences.

Keywords: Industry 4.0, IT/OT convergence, security assessment, smart manufacturing.

Resumo

Nos últimos 20 anos surgiram desenvolvimentos significativos na produção e desenvolvimento industrial, com novas tecnologias, redes e sistemas de produção emergentes devido ao desenvolvimento da internet e novos sistemas de produção adaptativos distribuídos. Essas arquiteturas resultaram em melhores atividades de serviço, novos modelos de negócios e aumento da demanda e oferta de bens, resultando em menos interações entre os participantes do sistema de produção.

A convergência de ambientes de IT/OT aumentou a complexidade e vulnerabilidade de redes OT/ICS anteriormente isoladas, e a crescente necessidade de expandir a automação na indústria cria um grande desafio em termos de segurança cibernética. Nesse contexto, como identificar atividades suspeitas, avaliar riscos e ajudar a prevenir paradas em um setor cada vez mais tecnológico?

Para esta tese, foram analisados dados recolhidos através de um inquérito online sobre o tema da convergência na indústria nacional, de forma a saber se este tema, na perspetiva dos profissionais, merece a atenção das organizações onde desenvolvem a sua atividade profissional com tecnologias de IT/OT. São identificados e analisados um conjunto de casos reais e as consequências de falhas graves de segurança ocorridas no período entre 2021 e 2023, cada vez mais comuns, com impacto na indústria à escala global.

Analisa-se a complexidade tecnológica que resulta da convergência entre tecnologias de informação (IT) e tecnologias operacionais (OT), destacando na prática os desafios para os quais a cibersegurança tem de se preparar de forma a desenvolver respostas eficazes e ajustadas ao contexto em análise. O maior desafio está na integração ”cibersegura”de tecnologias de computação centradas em dados nos sistemas de IT com a monitorização de eventos, de processos e de dispositivos nos sistemas OT.

Depois de analisar a complexidade das tecnologias IT/OT essenciais para a Indústria

4.0, recomenda-se uma leitura atenta do conjunto de frameworks descritos neste documento sobre boas práticas internacionalmente reconhecidas em cibersegurança. Bem como do acesso regular às bases de dados públicas, descritas neste documento, sobre padrões de risco e vulnerabilidades fundamentais essenciais para o desenvolvimento de uma estratégia de cibersegurança atualizada.

Por fim, são sugeridas, um conjunto de boas práticas para analisar, enquadrar, e aplicar na estratégia de cibersegurança de uma organização, para evitar situações de risco, monitorizando a tendência de incidentes de cibersegurança, de falhas de software conhecidas, de vulnerabilidades e riscos associados, que podem resultar, por exemplo, em ransomware com as suas consequências associadas.

Palavras-chave: Indústria 4.0, convergência de IT/OT, avaliação de segurança, manufatura inteligente.

Aknowledgements

Without the collaboration, support and dedication of many people, the development of this work would not have been possible. Therefore, I would like to express my sincere gratitude and appreciation to everyone who has made all of this possible. To my supervisor, Professor Paulo Costa, for his support, learning and encouragement to develop new ideas and explore new paths.

To the coordinator and Professor Pedro Pinto and to all the Master's professors for sharing and encouraging me to learn more about cybersecurity.

To all my colleagues for sharing experiences, knowledge and the strong team spirit that we have built over time, especially Pedro Sousa, Pedro Couto and Ricardo Silveira for the days of working together throughout the course.

To my friends Ricardo Andorinho and Paulo Afonso for their enormous patience and support in completing this challenge successfully.

To all my family and especially to my wife Sandra Pombal for their unconditional support.

I want to extend my sincere gratitude to everyone.

Contents

List of Figures

List of Tables

List of Abbreviations

5G 5th Generation Mobile Network

AI Artificial intelligence

ARP ARP Address Resolution Protocol

ATT&CK Adversarial Tactics, Techniques, and Common Knowledge

BYOD Bring Your Own Device

CPS Cyber-Physical System

CVE Common Vulnerabilities and Exposures

CWE Common Weakness Enumeration

DCS Distributed Control System

DDos Distributed Denial of Service

DNS DNS Domain Name System

ICS Industrial Control System

IEC International Electrotechnical Commission

IIoT Industrial Internet of Things

IoT Internet of Things

IP Internet Protocol

ISA International Society of Automation

ISO International Organization for Standardization

IT Information Technology

JNDI Java Naming and Directory Interface

LAN LAN Local Area Network

LDAP Lightweight directory access protocol

M2M Machine-to-Machine

MITM Man-in-the-Middle

ML Machine learning

NIST National Institute of Standards and Technology

OT Operational Technology

OWASP Open Web Application Security Project

RDP Remote Desktop Protocol

RMI The Java Remote Method Invocation

SCADA Supervisory Control and Data Acquisition System

WLAN Wireless LAN

WN Wireless Network

Chapter 1

Introduction

The Internet has a major impact on economic activity, with online business relationships becoming more common. It is an information and communication infrastructure, with scientific content being the primary production inputs and end products. Information and expertise are the primary production inputs and end products [8]. Industrial production and development have changed significantly in the last 20 years due to globalization, new technologies, and new production systems and network architectures. These systems are more complex and unpredictable, with fewer interactions between system participants [70]. It is important to frame the evolution of the industry in its four most relevant evolutionary stages, starting in 1780, the steam engine [112] and the mechanical loom [69] marked the first industrial era. After 1870 came the second era, which was marked by the use of electricity [88], the oil industry [45], and also large-scale production [185]. As of 1969, the third era appears with automation [154][8], resulting from advances in electronics, the emergence of new technologies, CAD/CAM systems [175] and also nuclear energy [62]. We currently live in the era of Industry 4.0 [95], where the following also stand out: Internet of Things (IoT) [105]; Cyber-Physical System (CPS) [87], Smart Factory [28]; among other technological solutions that will be analyzed throughout this document. The use of mobile, desktop, and online interfaces, as well as new multi-touch interaction modalities, has been embraced by industries [39]. A policy known as "bring your own device" (BYOD) is a set of guidelines that many businesses have implemented. It permits employees to use and connect personnel mobile devices, such as laptops, smartphones, tablets, and personal digital assistants, at work [127]. The IT revolution has resulted in a shift in business, with new concepts such as Industry 4.0, the Internet of Things, cloud-based systems, big data, and BYOD emerging. Security concerns remain a major concern for successful business [134]. The digital wave had a major impact on many industries, including manufacturing, marketing, supply chain management, energy management, and virtual reality (VR). Big data capabilities in the Internet of Things (IoT) have great promise for the manufacturing sector [73]. IoT enables connections between devices and people and is the central component of Industry 4.0. Briefly stated, the phrase "Industry 4.0" was originally used in a publication by the German government in November 2011 as a consequence of a project about a high-tech plan for 2020 [115].

1.1 Context

In industry, the concept of a smart factory is increasingly materializing, composed of cutting-edge physical and digital technologies to increase production and efficiency. Is the development of an integrated system for production processes that results from the fusion of various types of technologies, such as automation systems and robotics in the physical component, the Internet of Things (IoT), Cloud Computing and analysis of Big Data in the digital component [28]. A smart factory is an optimized connected manufacturing facility with smart machines, sensors, and robots that are seamlessly integrated with information system architecture to enable high levels of automation in transaction processing, real-time analytics that aid in decision-making, and the ability to produce finished goods at the lowest cost. Suppliers, operations, IT, planning, sales and marketing and customers benefit from what the ecosystem, i.e. smart factory, produces due to their close cooperation [73]. One of the key technologies for Industry 4.0 is the Internet of Things (IoT) because it speeds up, in real-time, the exchange of data between physical objects and digital processes beyond organizational boundaries, adapting production to the challenges of world globalization. It facilitates access to virtual prototyping processes, allowing interested parties to flexibly explore all available functionalities for the same vision of the functionalities and benefits of the product as a whole [115].

Another essential technology for Industry 4.0 is Cyber-Physical Systems (CPSs), which are systems that result from a harmonious and efficient integration of computing and physical components [26]. It opens up a set of possibilities in the different stages of the manufacturing process, such as [140]: Allow the development of resilient and context-sensitive control systems. Facilitate the application of corrective measures by creating bold configurations. To enhance computational processing in the detection, execution and evaluation of occurrences and results through advanced artificial intelligence algorithms using distributed architectures.

Industry 4.0 stands out for integrating new technological solutions into its operations, and production units, new technological solutions, such as Cloud Computing [11], the Internet of Things (IoT), the Blockchain [104] and Machine Learning (ML) [189]. ML, for example, enables predictive analytics to accelerate an organization's business intelligence maturity. Thus, productive units are developed, increasingly intelligent, integrated and interconnected in a network to different departments of one or several organizations physically dispersed around the globe, according to the nature of the business [194]. The following are key points from IBM's analysis of the technologies it believes are driving Industry 4.0 [188]:

- The Internet of Things (IoT) - It is an essential element of smart factories. On the factory floor, machines have sensors with IP addresses that allow them to communicate with other web-enabled devices. Collecting, analyzing and exchanging valuable data on a large scale is possible through this mechanization and connectivity.
- Cloud computing - Cloud computing is an essential part of any Industry 4.0 strategy. It enables faster and more cost-effective processing of the enormous amount of data that needs to be stored and analyzed. Small and medium-sized manufacturers can lower costs to a minimum or adjust costs in accordance with their needs as their business expands. To fully implement Smart manufacturing to be fully implemented, it is necessary to connect the engineering, supply chain, manufacturing, sales, distribution, and service systems.
- AI and machine learning - Manufacturing organizations can fully utilize the volume of information created not only on the factory floor but also across all of their business divisions, as well as from partners and other sources, thanks to AI and machine learning. Operations and business processes may be observable, predictable, and

automated with AI and machine learning. Industrial machinery, for instance, is prone to failure when in use. Using the data collected from these assets businesses can perform predictive maintenance based on machine learning algorithms, improving uptime and efficiency.

- Edge computing - Edge computing lowers security risks by keeping data near its origin. It takes the shortest time possible between the time that data is produced and when a response is required. Because real-time production operations require it, data analysis must be performed at the "edge," or where the data is generated. For instance, if a safety or quality issue is detected, the equipment may need to act quickly.

- Digital twin - Manufacturers can now create virtual twins of their production processes, assembly lines, factories, and supply chains thanks to Industrial 4.0. To build a digital twin the information is gathered from internet-connected sensors, equipment, PLCs, and other objects. Manufacturers can use digital twins to improve processes, increase output, and develop new products.

- Cybersecurity - Operational equipment (OT) connectivity in the factory or field creates new entry points for malicious attacks and malware while also speeding up production. When undergoing an Industry 4.0 digital transformation, it is crucial to take into account a cybersecurity strategy that covers both IT and OT hardware.

While organizations have to implement an increasing amount of measures to reduce the likelihood of unwanted occurrences and their consequences, attackers need to identify a timely vulnerability, if they have access to AI tools, they can gain an asymmetric warfare advantage [172]. In 2021, according to the IBM Security X-Force report [190], manufacturing was the most attacked industry, with an approximate growth of 5.5% compared to 2020, from 17.70% to 23.30%. And also to highlight, in 2021, the vector of infection in manufacturing organizations was vulnerability exploitation at 47% and phishing at 40%. There are about 14 billion connected IoT devices, according to the SAM Seamless Network's "2021 IoT Security Landscape" report [1], and by 2025 it is estimated that it could reach 31 billion. This report highlights the 900 million phishing attacks in 2021 related to

IoT. They indicate the data obtained from 730,000 networks and 132 million active IoT devices, among other sources, and an exhaustive analysis of different types of cyberattacks, such as DDoS attacks, phishing attacks, brute force attacks, etc.

1.2 Problem Statement and Motivation

In the industrial sector, with the technological transition to integrated information systems, data has become essential for processes related to the production and management of all inherent resources. This technological update, for example, through the development of solutions based on the Internet of Things [78] [197], generates greater complexity through the constant input and output of fundamental data for the planning, management and control of an industrial unit in the current context, for example, Logistics 4.0 [111]. Data input and output generate a variety of possible entry points that should be analyzed to assess their degree of vulnerability to external attacks [143]. The purpose of this thesis is to warn decision-makers who do not always have a realistic understanding of the increasing risks, beyond the losses that may be incalculable, of the significance of minimizing the potentially detrimental effects on business continuity. To raise awareness about the necessity of organizations with an industrial component reviewing and updating their cybersecurity strategies because, as described throughout this document, threats are alarmingly on the rise and affect all types of units, from the most basic to the most complex and interconnected, in a context of production that is becoming more decentralized and global, regardless of the industry. It is vital to implement good cybersecurity practices in the face of the resulting complexity of data networks between different devices, people and products [166]. Cybersecurity is increasingly essential throughout this technological ecosystem of Industry 4.0 due to the exponential use of IoT devices and embedded systems or CPS [123].

1.3 Objectives

This thesis has as its starting point a review of scientific publications on cyber attacks and their consequences for industry 4.0. "In the next step, it intends to analyze, evaluate and document in a final report:

- The effectiveness of its convergence between Information Technology (IT) and Operational Technology (OT).
- The strength of the overall cybersecurity strategy with a set of recommendations for improvement.

It is crucial to identify the flaws in systems that can be exploited, by attackers, such as SCADA systems, which are required to control equipment at various locations and collect and store operational data from automation systems and information technology systems [165]. Most importantly, designed to stop cyber threats from impairing the integrity, accessibility, and confidentiality of data and systems without affecting their regular operation [120]. IoT devices are targets for botnets [41], and it is essential to develop and implement, all the security procedures that allow reinforcing the security of this type of hardware, as well as internal and external controls, in order to reduce potential risks to external threats, and sometimes internal [94]. Countermeasures [7] are the materialization of a set of corrective measures defined as essential, to avoid threats, as well as to update resources at the hardware and software level.

1.4 Organization

Given the complexity of the topic under study, this thesis is organized into five research steps to produce a systematic study focused on the principles underlying industry 4.0. The following is an overview of the Structure of the five main pillars of this thesis:

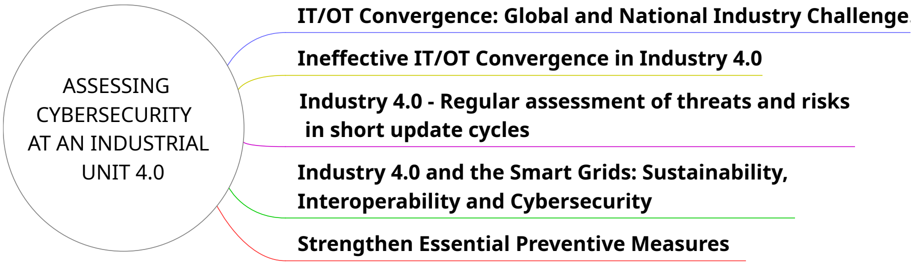
ASSESSING CYBERSECURITY AT AN INDUSTRIAL UNIT 4.0
IT/OT Convergence: Global and National Industry Challenge
Ineffective IT/OT Convergence in Industry 4.0
Industry 4.0 - Regular assessment of threats and risks in short update cycles
Industry 4.0 and the Smart Grids: Sustainability, Interoperability and Cybersecurity
Strengthen Essential Preventive Measures

Figure 1.1: Structure of the five main pillars of this thesis.

Throughout this thesis, scientific publications are reviewed on the industry 4.0 paradigm, but also on essential topics such as:

1. Industry 4.0 and IIoT enable data exchange and digital performance management, while IT/OT Cybersecurity focuses on data security and CPS integrity.

2. Cyberattacks are becoming more sophisticated and ICS environments are vulnerable to threats, so convergence between IT and OT is essential for industrial organizations to achieve efficiency, effectiveness and security.

3. Industry 4.0 is based on standards, reference architectures, and maturity models to guide the processes of integrating IT/OT security. Vulnerability identification, guidelines and standards, MITRE ATT&CK, Zero Trust Security are essential for organizations to prevent threats and attacks.

4. IoT, cloud computing, machine learning, and CPS enable Industry 4.0, and Smart Grids improve electric grids through the use of these technologies.

5. Organizations must take preventive measures to mitigate the risks of constant threats, such as ransomware, cyberattacks, security breaches, sabotage, and exploiting vulnerabilities.

Chapter 2

IT/OT Convergence: Global and National Industry Challenge.

2.1 Introduction

Manufacturing systems have been modified to an intelligent level in the context of Industry 4.0. In order to adapt production processes to a dynamic and international market, intelligent manufacturing makes use of cutting-edge information and manufacturing technology. Technologies provide direct contact with manufacturing systems, facilitating the speedy resolution of issues and the adoption of adaptive decisions [195]. With all this transformation, the intention is to improve the productive efficiency of the entire manufacturing value chain [14].

The goal of Industry 4.0 is to link manufacturing facilities to the Internet. Due to this hyperconnectivity, a significant amount of data from the value chain will be able to be collected and stored for a variety of purposes, including data collecting and storage for traceability and digital performance management. Because of the way heterogeneous equipment is integrated into the industrial cyber environment, cybersecurity considerations must be incorporated into their design approach [120]. The term "industrial IoT" describes a factory that is intelligent, automated, and completely linked. However, due to its susceptibility to cyberthreat vectors, a lack of standardization, and interoperability concerns, the IT/OT ICS environment has gaps. Modern technology such as 5G underpins IIoT M2M communication, which requires complex approaches to provide sufficient levels of data security. To achieve this, a fully integrated vertical model must replace the hierarchical models in use today. However, the transformation to a fully connected vertical model, from traditional hierarchical models, results in greater exposure to cyber-attack vectors aimed at exploiting gaps in interoperability and standardization at the level of the Industrial Control System (ICS) [41].

2.2 Related Work

A new industrial world emerges, in addition to the constant connectivity between devices, new standards and protocols, allowing the constant exchange of data through online and decentralized communication [114]. The authors, in ref., emphasize the differences in IT and OT priorities, that is, IT protects data, and prioritizes confidentiality, integrity and availability [44]. It also has a high frequency of updates and uses standardized operating systems and protocols. The cybercriminals' motivation is monetization, and the mission of their specific cyberattacks is oriented towards the traditional IT programming languages, frameworks and tools that developers use to develop applications in use in organizations. OT stands out for protecting assets, prioritizing the availability, integrity and confidentiality of devices and their systems. It reveals a low frequency of updates and uses proprietary operating systems and protocols [121] [5].

The availability of goods and/or services from a targeted business, or even the entire platform for financial exchange, can be impacted by cybercriminals, which can impact the stock prices of the related companies. Numerous businesses that provide their clients with services risk becoming a victim. DDoS attacks are a popular method used by cybercriminals to carry out market manipulation attacks. Despite not suffering any physical harm in this kind of attack, the victim may still be negatively impacted. The motivation of cybercriminals is the interruption of proper functioning, with the mission of cyberattacks being oriented towards a certain type of productive sector [158].

When physical inputs and controlled physical actions modify data in the real world in real-time, OT/ICS assets are monitoring and managing that data. Data in transit or at rest are the main focus of traditional IT assets. This is so because OT/ICS concentrates more on the physical and safety world, whereas IT focuses more on the digital data world [174].

The primary concern of using CPS in manufacturing is to produce improved products by shortening production time. Automation and process/machine reconfiguration are to be ensured dynamically satisfying a common standard. Improve production includes the factors of quality control, productivity, visualization, monitoring, production time, PLC, zero defect, safety, risk, and improve automation [39].

In this new paradigm, devices, in an industrial environment, gradually add intelligence, communicating with each other, in the ecosystems where they are integrated, thus giving rise to the Industrial Internet of Things (IIoT) [41]. Automation is increasingly the result of Machine-to-Machine (M2M) communication, established between devices, improving the reliability of data to be integrated into processes, from production to distribution [133].

2.3 The Complexity of Cyber-Physical Systems

In addition to being complex, Cyber-Physical Systems allow the development and integration of resilient and context-sensitive control systems into production processes. As a result, through feedback loops between physical and cybernetic components, greater efficiency is achieved in monitoring and control processes. There are CPS with different characteristics, such as [147]:

- Embedded systems - They are subsystems developed for specific functions, such as a microprocessor inserted in a coffee machine, which is made up of hardware and software. The efficiency of production cycles depends on the control of industrial machinery, i.e., on industrial automation.

- Real-time systems - The calculation time is crucial for safety-critical systems since it affects how sure we can be that the system is operating correctly. Developers may describe the timing requirements for their systems with the use of real-time programming languages, and real-time operating systems (RTOS) to ensure that tasks from applications are accepted and completed within the specified time frame.

- Network protocols - Many critical infrastructures such as power systems and SCADA systems communicate with each other over IP-compatible networks. In the past two decades, communications between different parts of the system have moved from serial communications to IP-compatible networks.

- Wireless (sensor networks) - Wireless communications for embedded systems attracted significant attention from the research community in the early 2000s in the form of sensor networks. While most long-distance communications are done over wired networks, wireless networks are a common characteristic of CPSs. Building networks on top of low-powered, lossy wireless links presents a challenge because traditional routing concepts like the "hop distance" to a destination are no longer relevant. Instead, link quality metrics, such as the expected number of packet transmission attempts before a one-hop transmission succeeds are more reliable. Popular embedded wireless protocols in the consumer IoT market include Bluetooth, Bluetooth Low Energy (BLE), ZigBee, and Z-Wave.

- Control - Feedback control systems have been around for more than 200 years, dating back to the introduction of the steam governor in 1788. Initially, analogue sensing, and analogue control, were used to create control systems, which meant that the control logic was embodied in an electrical circuit. A continuous-time physical process might be seamlessly integrated with control signals thanks to analogue systems. Within the scope of control, there are three sub-features to be highlighted:

  - Discrete-time control: With the development of digital electronics and the microprocessor, work on discrete-time control became necessary since computers and microprocessors are unable to operate a system in continuous time because sensing and actuation signals must be sampled at discrete time intervals

  - Networked-controlled systems: With the development of digital electronics and the microprocessor, work on discrete-time control was necessary since computers and microprocessors are unable to operate a system in continuous time because sensing and actuation signals must be sampled at discrete time intervals.

  - Hybrid systems: The study of hybrid systems is a new attempt to bring together the conventional computational models of physical systems (like finite-state machines) and physical systems (like differential equations). As an insight into

> how integrating models of computing and models of physical systems might result in new theories that allow us to reason about the features of cyber- and physical-controlled systems, hybrid systems were a primary driving force behind the development of a CPS research program.

Security and privacy concerns are high because the disruption of critical infrastructure such as power, water and transportation can have a significant impact on public health, safety and economic losses.

2.4 The Cyber-Physical Systems domains to be protected

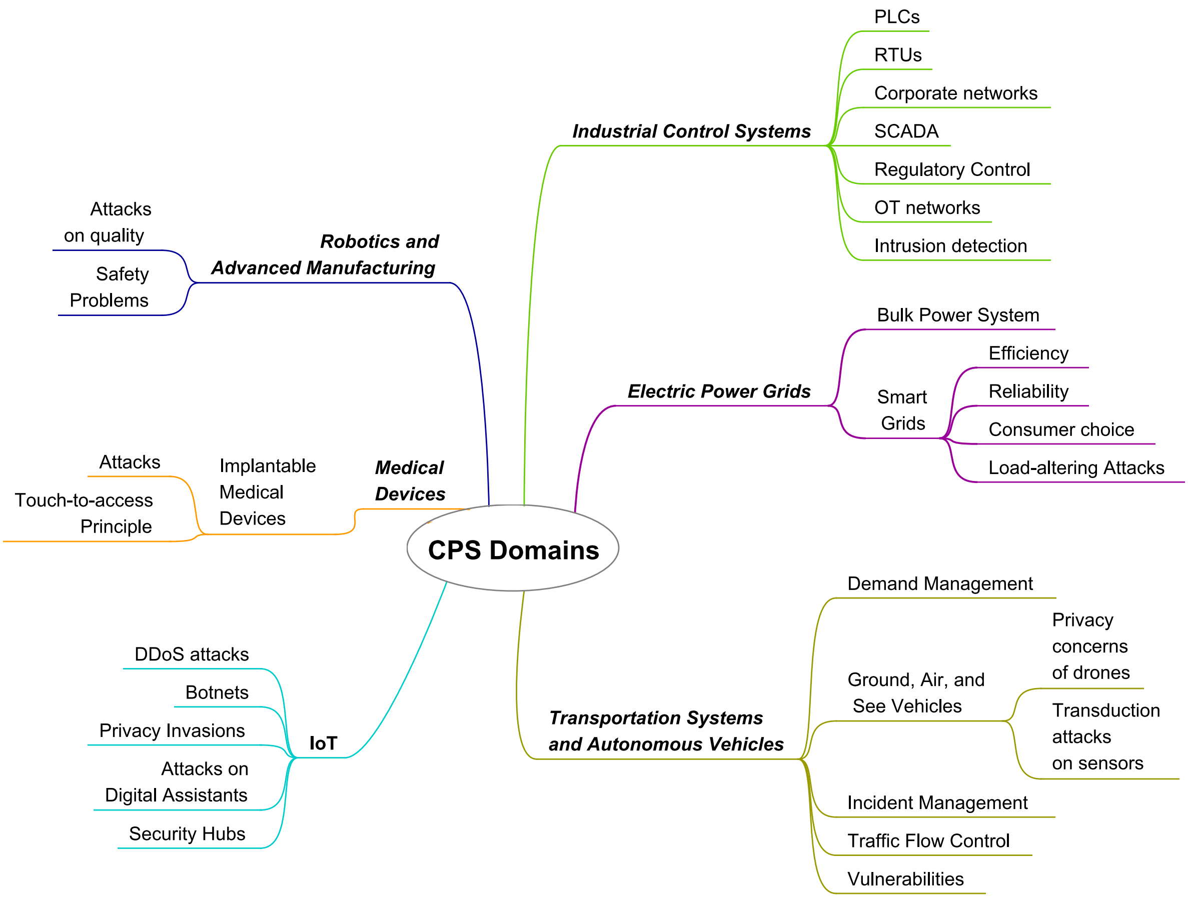

Figure 2.1: Cybok six CPS domains from Cyber-Physical Systems Security Knowledge Area.

A CPS's weakest link can be identified by an attacker, who can then focus on its most exposed parts to cause the greatest amount of system functionality loss. Concerns with security and safety must be considered in the CPS risk assessment. To address all potential failures and threats in a thorough and comprehensive manner, developing a fully integrated risk assessment approach is essential. While safety analysts rely on consolidated approaches to identify, analyze and take decisions to counteract hazards, cyber threats identification and analysis methods (including defend-attack models) are still under development. Cyber threats' impact on CPS functionality and the maximization of CPS reliability and survivability are sought by defenders in making decisions on the allocation of defensive resources [183]. Industrial control systems are one of the six CPS domains, according to the Cyber-Physical Systems Security Knowledge Area, the others being.

Exploring the Industrial Control Systems domain is essential to further deepen your knowledge and this is because it represents a broad range of physically linked, networked information technology systems. To remotely monitor the pressure and flow of gas pipelines, the oil and gas sector employs integrated control systems. Water utilities are able to remotely regulate the well pumps and check the levels of the wells. Control systems feature a tiered hierarchy that is used to divide the network and enforce access control. The Corporate networks, the upper layers control the business logistics system using traditional information technology, such as computers, operating systems, and related software. They enable management of the plant's basic production schedule, material usage, shipment and inventory levels, as plant performance, and maintain data for data-driven analysis, such as predictive maintenance. The PLCs are a key component in the automation of processes and factories. It has a special purpose that can handle input/output signals and perform serial communications and is used to execute control programs, particularly those involving complex interlocking sequences and control logic. OEMs can integrate PLCs into machines or process equipment, use them stand-alone in local control settings, or connect them to the network to control systems. And the Remote telemetry units and remote control units are two types of remote (RTUs) terminal units that can be used to connect physical items with distributed control systems (DCS) or SCADA systems. The SCADA is a system used in manufacturing to provide regulatory or machine control over a process area or work cell to collect measurements of process variables and machine status. Regulatory Control is essential because it involves instrumentation in the field, such as sensors such as thermometers, tachometers and also actuators such as pumps and valves. The OT Networks, the fundamental systems in management and control, usually in a manufacturing environment, such as the SCN and FCN networks, have different communication needs. While SCN may accept delays of up to a few seconds, FCN usually demands orders of magnitude smaller communication delays, often between a few seconds and a few minutes. Intrusion detection makes use of custom network security monitors to industry standards and physics-based anomaly detection is an important subject of study for protection control systems. The types of attacks that can be found depend very much on the layer where we follow the physics of the system.

2.5 IT/OT Cybersecurity: The Impact Of Changes In The Industry

For many years, the upper tiers of control networks have deployed conventional off-the-shelf operating systems, frequently used in office settings, to assist in automating engineering operations. They should be treated, managed, maintained, and secured as OT/ICS assets because they have a mission of engineering and safety, as opposed to standard IT assets. One common fallacy is the perception that ICS environments can easily adopt IT security procedures. Even though there is a wealth of knowledge accessible in IT security, "paste and forwarding" IT security technologies, processes, and best practices into an ICS could have negative or disastrous effects on production and safety [174].

With the increasing sophistication of cyberattacks [46], organizations need to implement active, rather than reactive, cybersecurity programs [11] [97] tailored to their industry context, including disaster recovery and contingency plans [41]. Attacks carried out, such as ransomware, by groups, some of them backed by governments [120], undermine trust in cybersecurity programs [51] [53].

The impact of various trends such as remote monitoring, the use of different types of cloud computing applications [34], and the transition to digital business processes, accelerate the transformation of the industrial context and accelerate the convergence of IT/OT [32]. All of this has a major impact not only on the safety of work teams but as well as on the ability to guarantee critical infrastructure systems and services [80], such as for energy production units or smart cities [192].

The corporate system providers themselves are migrating to cloud computing environments, providing services in the cloud [34], either to their customers after authentication to ensure security [29]. The IT / OT convergence has a critical mission in the design and implementation, of a common strategy [41] to focus on data security, CPS integrity, effective implementation of keys for device pairing, as well as the development of management of installed and operating devices [32].

The newly discovered weaknesses can be used by individuals or groups. Although there are some glaring differences between the two worlds, convergence is not the issue. The fundamentally different priorities of OT and IT, which result in a discontinuity in the cyber security space are what constitute a significant issue. People or groups looking to take advantage of these recently discovered vulnerabilities have emerged as a result of this exposure [174].

2.6 IT/OT Convergence In The National Context: Online Survey

Due to the relevance of the theme of convergence at a global level, the curiosity arose to explore and analyze it a little more through an exploratory study based on the individual experience of professionals in this theme in the Portuguese context. About thirty IT and OT professionals linked to the national industrial sector were contacted. An online form was sent to all elements of this group, of which twenty-four responded in good time, that is, within the pre-established period of fifteen days. It was an important opportunity to gain insights through the responses collected from professionals in the field. Qualitative data was exclusively obtained using an online questionnaire consisting of five questions set inspired by the SANS 2019 State of OT/ICS Cybersecurity Survey report [53]. This approach is about collecting data on whether the respective organizations where they work, implemented and promoted a clear strategy of convergence between IT/OT technologies. Then, the results obtained are presented, as well as the respective questions, which were the following:

Question nº1 The first question asked was: "Does your organization carry out a security assessment or audit of control systems and control systems networks?" The most interesting results obtained are, as shown in table 1, around 83% answered "yes", 9% answered "no" and 8% answered "I don't know".

Yes	83%
No	9%
Perhaps	0%
I don't know	8%
In the near future	0%

Table 2.1: Results in the percentage of responses to the first question.

Question nº2 The second question asked was: "Does your organization invest in cybersecurity awareness programs for IT, OT and/or hybrid IT / OT staff?". The results obtained, as shown in table 2, about 88% answered "yes", 4% answered "no", 4% answered "I don't know" and finally 4% answered "In the near future".

Yes	88%
No	4%
Perhaps	0%
I don't know	4%
In the near future	5%

Table 2.2: Results in the percentage of responses to the second question.

Question nº3 The third question asked was: " Does your organization promote strategies to unite IT and OT initiatives?". The results obtained, as shown in table 3, about 67% answered "yes", 4% answered "no", 8% answered "Perhaps", 17% answered "I don't know" and 4% answered "In the near future".

Yes	67%
No	4%
Perhaps	8%
I don't know	17%
In the near future	4%

Table 2.3: Results in the percentage of responses to the third question.

Question nº4 The fourth question asked was: " Does your organization implement anomaly and intrusion detection tools on control system networks?". The results obtained, as shown in table 4, about 88% answered ”Yes”, 4% answered ”No”, 4% answered ”Perhaps” and 4% answered ”I don’t know”.

Yes	88%
No	4%
Perhaps	4%
I don’t know	4%
In the near future	0%

Table 2.4: Results in the percentage of responses to the fourth question.

Question nº5 The fifth question, and the last, was: ”Does your organization invest in cybersecurity education and training for IT, OT and/or hybrid IT / OT teams?”. The results obtained, as shown in table 5, about 83% answered ”yes”, 13% answered ”no” and 4% answered ”I don’t know”.

Yes	83%
No	13%
Perhaps	0%
I don’t know	4%
In the near future	0%

Table 2.5: Results in the percentage of responses to the fifth question.

2.7 Online Survey Conclusions

Upon closer examination, it can be seen that the ”yes” response remained above 80%, except for the third question, which obtained only 67%. The security assessment, or audit, of control systems and networks, is ”unknown” to about 17% of those who responded, as well as a ”maybe” of 8% of the answers. In this strand, we have approximately 25% professionals who are somehow unaware of whether or not the organization is active in assessing or auditing the security of its systems and networks. Another aspect to consider is the result obtained by the ”no” in question 5 about the investment in education, and training, in cyber security for teams, which stands at 13%, as well as we can also analyze the 4% who do not know if this is true in practice. In other words, we deduce that 17% do not benefit for some reason, or specific criteria, from these types of training programs that are essential in an area such as cybersecurity, naturally suited to their respective roles and responsibilities in the organization. It was an opportunity to gain insights through responses collected from professionals in the field. After reading these data, some questions arise that must be analyzed by those responsible if, in the organization itself, these questions are getting a positive and effective response in the practical and functional plan. Some of these questions are:

- Can the awareness of your human resources about the cybersecurity policies implemented in the organization be improved?
- Can the organization involve professionals more in the development of conversion strategies, or integration, between IT and OT?
- Are cybersecurity education and training programs for internal teams available in a tailored and affordable way for everyone?

These questions can be included in a preliminary issue survey plan, recurrently and systematically as part of an internal continuous improvement process.

Although the questionnaire has only five questions, which is a limitation when the objective is to obtain a broader vision of convergence, in this specific case, it appears as a first step so that in the future, with the experience obtained in this initial approach, it will be a basis of knowledge to evolve into more complex and in-depth research work on this topic in a specific industrial sector.

Chapter 3

Ineffective IT/OT Convergence in Industry 4.0

3.1 Introduction

The industry is modernizing, and throughout this process, it has been the target of ongoing cyberattacks that aim to take advantage of its flaws and misunderstandings about the people who work in organizations in order to make it more valuable as a target [121]. In practice, the chances of being victims of cyber threats grow and sometimes result from complex strategies of data theft [56], sabotage of critical infrastructure [54], and ransoms in cryptocurrencies [196], among many other cyber threats. The constant connection between industries and their production chains in the global economy makes them more exposed to increasingly sophisticated cyberattacks [57]. The main types of threats that can be part of attacks are viruses, worms, Trojans, spyware and ransomware [84]. The perception that ICS environments can easily adopt IT security procedures can prove to be an inefficient and ineffective approach, here are some examples [174]:

- Systems for network and/or endpoint-based intrusion prevention may reject valid engineering commands that have been mistakenly labelled as harmful. These could include genuine, valid safety or real-time control system orders that are necessary for a facility to function, blocked and upcoming operations, and potential safety protocols.

- A typical antivirus system might mistakenly prevent an engineering application or process from running or carrying out a particular function because of a flawed antivirus signature or heuristic-based rule, which would obstruct the view, control, or safety of a control system.
- Devices that improperly interrupt IT-type scanning software could be used for vulnerability scanning, rendering engineering hardware unresponsive and adversely affecting the dependability and performance of control elements, such as an active safety instrumented system.

3.2 Threats to Cyber-Physical Systems

There is currently a wide range of devices in operation in industry 4.0, which in recent years has revealed a high number of vulnerabilities in many endpoints, which can be exploited by hackers, becoming potential targets with unpredictable consequences in terms of integrity, confidentiality and availability, of the assets of an organization [32].

The heart of all medical equipment, energy systems, armament systems, and transportation management are CPSs. Particularly in crucial national infrastructures like intelligent transportation systems, water and waste-water treatment, oil and natural gas distribution, and electric power distribution, Industrial Control Systems systems play a crucial role. Attacks on the electrical grid, for instance, might result in blackouts, which can have interdependent cascade consequences on other crucial infrastructures like computer networks, medical systems, or water systems, potentially having devastating impacts on our society's economy and safety [147].

Big data and sensor technology, artificial intelligence, physical automation, remote operations, cloud computing, and analytics have the potential to improve productivity and production, which is what is driving convergence. Operators must improve network connectivity and access to both IT and OT systems using Ethernet, WI-FI, and TCP/IP standards in order to make all of this possible [121].

The Cyber Security Body of Knowledge presents eight examples of CPS attacks, which are as follows [147]:

1. When a sensor is compromised, an attacker can intentionally tamper with the sensor

data or inject false sensor signals that cause the system control logic to act on malicious data. This happens, for instance, when the attacker has the sensor key material or the sensor data is not authenticated.

2. An attacker in the line of communication between the sensor and the controller, who can hinder or even stop the information being sent from the sensors to the controller, preventing the controller from seeing the system and forcing it to function with outdated information. Denial of service attacks on sensors and stale data attacks are two examples that result from this type of attack.

3. Tampered control signals can be sent to actuators by an attacker who takes over the controller.

4. An attacker can cause a denial of control of the system, by generating a delay or even blocking any control command, in practice, it is a denial of service for the actuators.

5. Controller attacks can result in zero dynamics attacks, which are different from those that can compromise actuators. This type of attack can allow the performing of control actions that are not intended by the controller.

6. Blended attack, in which an attacker can physically attack the system to cause physical damage to a piece of infrastructure and perform a cyber attack as part of their strategy.

7. SCADA system can be subject to an attack, for instance, if a third party obstructs or delays communications to and from the supervisory control system or configuration devices.

8. An attacker can take control of the SCADA system or configuration devices, can impersonate them and send malicious commands or configuration changes to the controller. Two practical examples of cyber-attacks are the power grid in Ukraine, the SCADA system control room where computers infiltrated, or the cyber-attacks compromising the configuration of medical devices.

3.3 Cyber attacks on industry and their consequences

The challenges generated by the specific context of each industry put us before the complexity in the integration of different technologies, whether Information Technology (IT), Operational Technology (OT), or both. Convergence between OT and IT for the industry is increasingly vital to obtain efficiency, effectiveness and security from the different technological solutions adopted [32]. A question naturally emerges in this cybersecurity context, which is: ”What consequences can result from an ineffective IT/OT convergence for an industrial organization?”

3.3.1 Real examples of industry cyberattacks in 2021

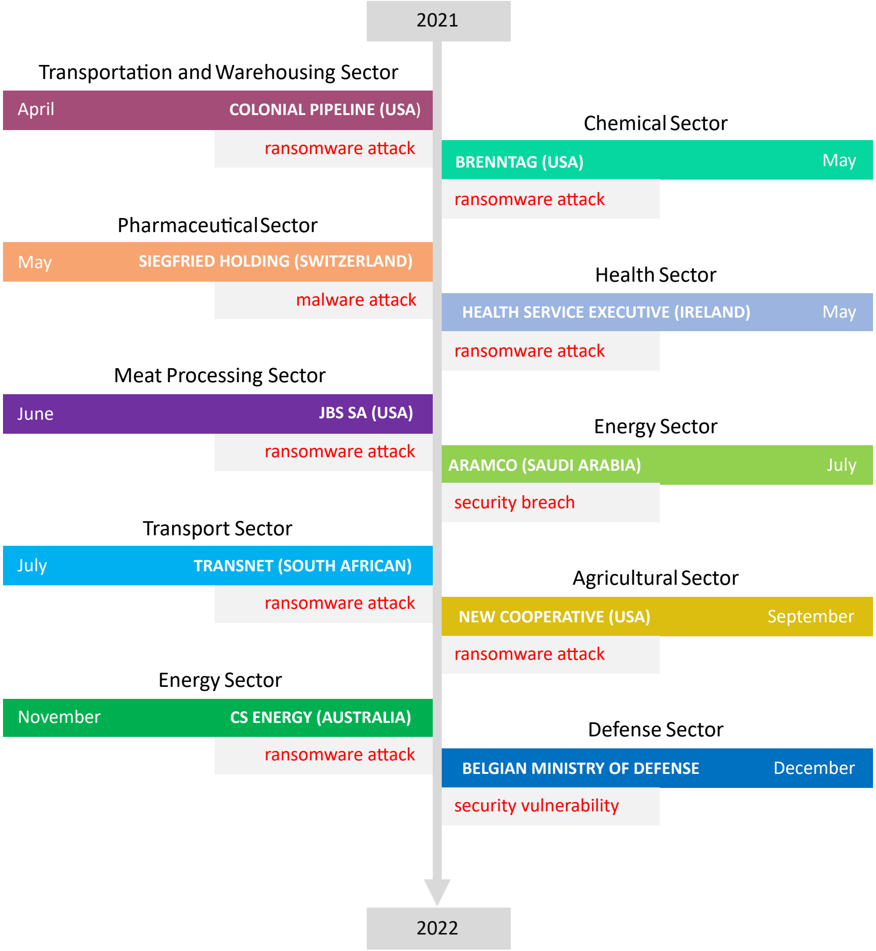

Figure 3.1: Real examples of industry cyberattacks in 2021

In 2021, a series of cyberattacks with a significant impact took place that resulted in consequences not only for the targeted industrial organizations but also for their partners and customers in several economic sectors. Next, some real cases that happened throughout the year are listed:

1. Transportation and Warehousing sector - In April, the largest US pipeline operator, Colonial Pipeline, suffered a ransomware attack carried out by the DarkSide group [186], suspected of eastern European origin, offering ransomware-as-a-service attacks [46]. As a consequence, it led to a shortage at gas stations along the east coast of the country, as its fuel distribution operations were suspended, forcing the company to shut down the pipeline and some of the organization's systems [178]. Another impact was seen in the logistics chain to improve flexibility in the distribution and supply of fuel, temporarily allowing the drivers of fuel transport trucks some compliance with the regulations in force [89].

2. Chemical distribution and manufacturing sector - In May, Brenntag's North American division suffered a ransomware attack [21], carried out by elements of the DarkSide group that claimed to have seized 150GB of unencrypted data and encrypted devices on the network. Brenntag, two days after the attack, to contain the threat, disconnected the affected systems from the network and hired external services specialized in cybersecurity and forensic auditing to investigate vulnerabilities in its systems, and report what happened to the authorities. About 6700 people were notified, by Brenntag, to verify suspicious bank movements or attempts at identity theft and fraud. Upon investigation, experts found no evidence that the stolen data was used for fraudulent purposes.

3. Pharmaceutical sector - In May, Siegfried Holding, based in Zofingen, Switzerland, with a presence in 7 countries, suffered a malware attack [27] on the IT network, detected through internal monitoring systems, according to information from the company itself. It is a manufacturing partner for the Covid BioNTech vaccine developed by pharmaceutical Pfizer at Siegfried's production facility in Hameln, Germany, affected by the attack. As a consequence, production was interrupted in several units of the group. An audit was carried out on all IT systems, and the manufacturing processes, of the various units, were gradually restored.

4. Public health services - In May, the Health Service Executive (HSE) in Ireland suf-

fered a Ransomware attack, allegedly carried out by Conti's group. This group is based in Russia, and runs Ransomware as a service (RaaS), with a primary focus on attacks on critical infrastructure networks and large enterprises. The group, in exchange for a digital key to unlock HSE servers, demanded 20 million dollars in cryptocurrencies. As a result of the attack, the HSE system was shut down, having a negative impact on hospital services in terms of diagnoses, the cancellation of appointments and disrupting the normal functioning of COVID-19 testing campaigns.

5. Meat Processing Sector - In June, the largest meat producer in the world, JBS SA, present in 20 countries and based in Sao Paulo, suffered a ransomware attack [125] in 2021 is presumed that it was carried out by the REvil or Sodinokibi group, which affected its operations in the USA and Australia. In these markets, as a result, several of the company's meat industrial units were affected in their normal operation, leading to the interruption of their operations temporarily. In the global business dimension of JBS, this situation causes constraints not only in distribution but in the entire economic cycle that is from producers to final consumers and an impact on exports that trigger interruptions in supply chains in these markets. JBS USA paid a ransom equivalent to 11 million dollars.

6. Energy Sector - In July, Aramco, an oil company in Saudi Arabia, which is the largest global oil company by revenue, suffered a cyberattack [43]. As a result, and according to the company, the attack resulted in data theft from an Aramco partner. On the Dark Web, a hacker published a post in which he claimed to have stolen one terabyte of confidential data from employees, customers, various types of documents and the location of oil refineries and demanded a ransom of 50 million dollars. According to the oil company, the attack had no impact on its operations.

7. Transport Sector - In July, Transnet, which is a South African state-owned logistics company based in Johannesburg, according to the company, suffered [137] "an act of cyberattack, security breach and sabotage". This event had an impact on the proper functioning of several container terminals, causing delays and disrupting the normal flow of imports and exports. About 60% of all South African trade passes through the Port of Durban, after the attack, it is processing only 10% of its capacity.

8. Agricultural Sector - In September, New Cooperative, based in Fort Dodge, Iowa, USA, suffered a ransomware attack [67] carried out by the BlackMatter hacking group. This cooperative has 93 member companies, a total of 226 employees and generates around 480 million dollars in sales. Hacking group BlackMatter, demanding payment of 5.9 million dollars in cryptocurrencies, threatening to expose various types of documents, as well as the source code of its ground mapping technology, according to the same as about a terabyte of information in exchange for a ransom or payment of the ransom in cryptocurrencies. As a consequence, the cooperative disconnected its computer network to isolate the threat, as well as soil mapping software, which is a control system to optimize irrigation and fertilization. Another consequence was the manual registration on paper of grain loads delivered by farmers to their cooperatives to circumvent the non-functioning of the registration software used. Being a critical infrastructure, an attack on its systems can interfere with the feeding schedule of more than 10 million animals and processes of approximately 40% of the country's grain production.

9. Energy Sector - In November, CS Energy, a company from Queensland, Australia, whose main business is the generation and sale of electricity in the National Electricity Market, was attacked by ransomware [81]. This company has more than 500 employees and operates two units producing more than 30% of Queensland's electricity with a commercial portfolio of 3,535 megawatts. As a consequence, the company reacted to the incident that affected the corporate network by isolating it from other internal networks notifying state and federal agencies and implementing the business continuity and disaster recovery plan.

10. Defense Sector - In December, the Belgian Ministry of Defense detected a cyber-attack because the attackers triggered a vulnerability [159] in the Apache Log4j software [13], which is a Java library for logging error messages in applications. As a consequence, the Belgian Ministry of Defense, as a precaution, disconnected parts of its computer network. This type of vulnerability allows when a device is running certain versions of Log4j 2, attackers can remotely take control of that device online.

3.3.2 Real examples of industry cyberattacks in 2022

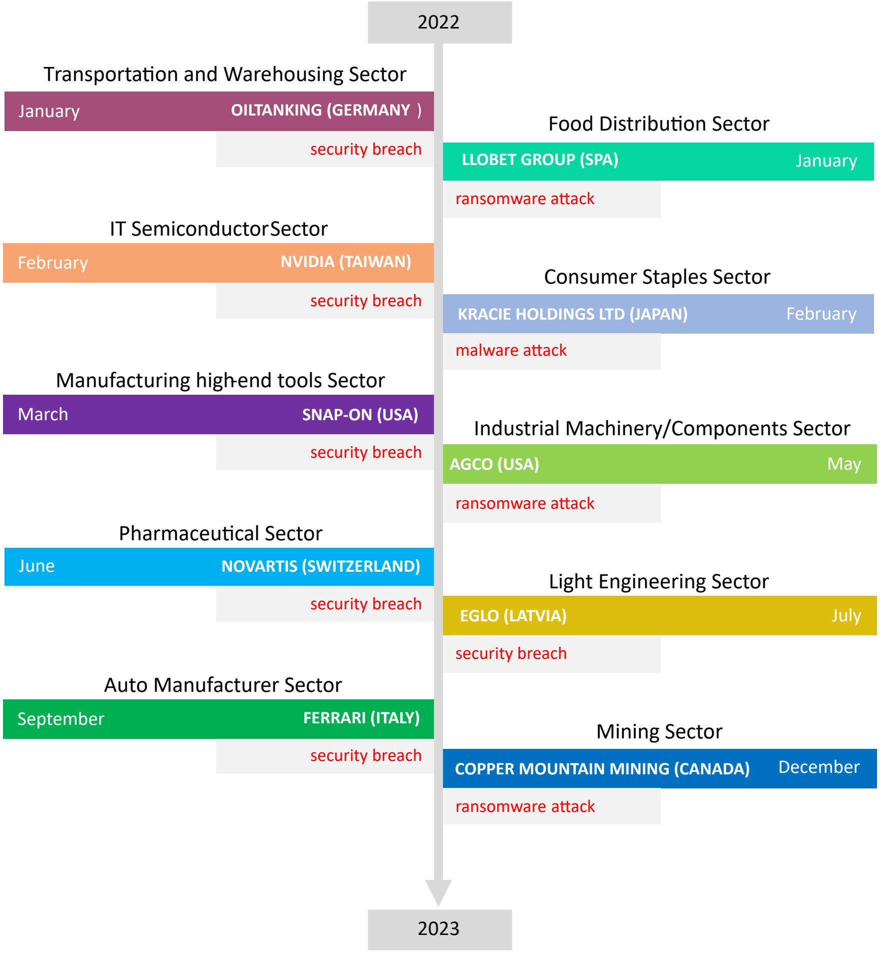

Figure 3.2: Real examples of industry cyberattacks in 2022

High-impact cyberattacks continued their pattern from the previous year, with negative effects on the targeted industrial organizations but also their partners and clients in numerous economic sectors. The following are some actual incidents that took place in 2022:

1. Transportation and Warehousing sector - In January, the German business Oiltanking recognized that one of its systems had been impacted by a cyber incident. An oil terminal breach occurred at several European ports, in a total of seventeen: eleven were located in Germany, and six in Belgium and the Netherlands. The cyber attacks made it difficult for the terminals to load and unload the oil. Due to the attack, Oiltanking has invoked an extension of time, making it impossible for them to fulfil their obligations to supply oil as per their contracts [116]. The energy infrastructure

is becoming more and more vulnerable to cyberattacks, which are similar to the ransomware attack on the American oil pipeline company Colonial Pipeline.

2. The Food Distribution sector - In January, Los Mossos d'Esquadra is investigating a cyberattack on the Llobet group (supermarkets), which has blocked all operations and asked for a ransom [103]. The company has not agreed to pay what the 'hackers' ask, and is in the hands of companies specializing in cyberattacks. During the weekend, the warehouse experienced frenetic activity to re-introduce product by product in a new computer system.

3. IT Semiconductors sector - In February, Over 70,000 Nvidia employees' usernames and cryptographic hashes were stolen during an attack [124] earlier this year that cost the microchip manufacturer Nvidia one terabyte of data. The hack was blamed on the Lapsus$ ransomware group. The criminal gang first demanded the removal of a feature that makes Nvidia graphics cards less desirable for cryptocurrency mining and later modified the demand to require open-source graphics drivers for all future cards. Unless Nvidia complied with their demands, the gang threatened to release the stolen data.

4. Consumer Staples sector - In February, Kracie Holdings Ltd, a Japanese supplier of pharmaceuticals, cosmetics and foodstuffs, confirmed that some of the group's machines were infected [128] with the computer virus Emotet after receiving suspicious emails from a third party that appeared to be a member of the group. A group employee's name appears as the sender of the questionable email. Anyone who opened files linked to these shady emails could become infected with a computer virus, and the data on that computer could then be unlawfully accessed. After informing about what happened, promised to make all reasonable efforts to prevent the spread of damage and internally encourage the reinforcement of information security procedures.

5. Transportation industry sector - In March, when High-end tools manufacturer Snap-on discovered suspicious activity in their network and had to shut down all of their systems as a result, they discovered a data breach [162]. Snap-on, from the USA, is a

leading producer and developer of tools, software, and diagnostic services used by the transportation industry. They think that the incident involved information about franchisees and associates, including names, Social Security numbers, birthdates, and employee ID numbers. For those who are impacted, the company is providing a complimentary identity theft protection service for a year.

6. Industrial Machinery/Components sector - In May, AGCO, an American agricultural machinery manufacturer, has been affected by a ransomware attack [6], which caused it to close some of its manufacturing facilities and send its employees home. The company is still investigating the attacks and has not identified which ransomware family it was attacked by. It expects its business operations to be "adversely affected" for several days and could take "potentially longer" to resume all services depending on how successfully it fixes its systems.

7. Pharmaceutical sector - In June, Novartis was the victim of an extortion attack [136] by the Industrial Spy hacker group, which sells data obtained from infected companies. According to Novartis, it did not compromise any relevant information. Encryption was not used at the event according to the available information. Data allegedly taken from Novartis was put up for sale by the hacking gang for $500,000 in bitcoins.

8. Light engineering sector - In July, EGLO Latvia's systems were the target of a cyberattack. After being informed of the occurrence, the cybersecurity team was able to immediately isolate the system. However, some of the systems have been disabled for security reasons. Steps were taken to reduce the impact on customers and partners of systemic issues affecting orders and deliveries.

9. Auto Manufacturer sector - In September, Ferrari, the Italian luxury car maker, was hit by ransomware [52]. The ransomware gang RansomEXX's dark web leak website published data from the Ferrari website. Internal papers, databases, maintenance instructions, and other materials are allegedly in possession of hackers. In less than a year, hackers have stolen papers from Ferrari twice, with the most recent incident being the leak.

10. Mining sector- In December, The British Columbia-based Canadian Copper Mountain Mining Corporation (CMMC) disclosed that a ransomware attack [25] negatively affected its operations. In order to contain the incident, CMMC shut down other components and isolated the affected systems in order to assess the impact of the ransomware attack. CMMC, an 18,000-acre claim that is partially owned by Mitsubishi Materials Corporation, produces 100 million pounds of copper on average annually and has an estimated mineral reserve capacity for 32 more years.

3.3.3 Real examples of industry cyberattacks in 2023 (January and February)

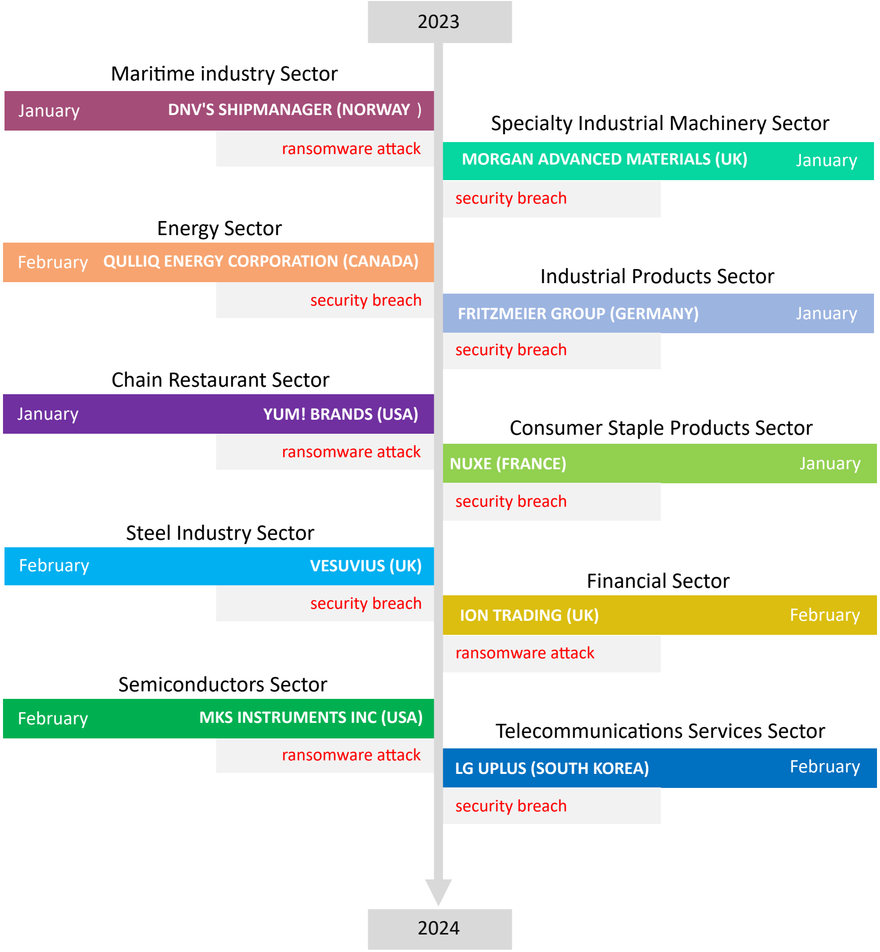

Figure 3.3: Real examples of industry cyberattacks in January and February 2023.

In 2023, the year is still February a series of cyberattacks have already been reported. Repeated events similar to those in the attacks previously mentioned, with varying degrees of impact on the operations of the targeted businesses, and occasionally with implications that also affect their clients and partners regardless of their industry. These are a few actual incidents that took place in January and February:

1. Maritime industry sector - In January, DNV's ShipManager (IT software) from Norway, servers fell victim to a ransomware cyberattack [150]. More than 1,000 boats operated by around 70 customers were impacted. In reaction to the situation, DNV experts promptly shut down the servers. The vessel's ability to function was not affected by the attack. The attack, which has also been reported to the police and other relevant authorities, is being investigated by external technical experts. Furthermore, the German Cyber Security Authority, the Norwegian Data Protection Authority (DPA) and the Norwegian National Security Authority have been notified.

2. Industry Specialty Industrial Machinery sector - In January, Morgan Advanced Materials, in the UK, following the discovery of illegal activity [118] on its network, notified through an official alert that it actively addressed the cybersecurity issue. They initiated an investigation with their professional support services and implemented their incident response procedures. The IT infrastructure implemented preventive measures to contain the situation and measures to correct and restore services.

3. Energy Sector -In January, Qulliq Energy Corporation (QEC), a Canadian territorial corporation, was targeted in an illegal cyberattack [142]. QEC's network was breached, and the corporation took immediate action to contain the situation. Out of an abundance of caution, all QEC customers are encouraged to take steps to protect personal information. Customers should monitor bank and credit card accounts regularly for unusual activity. Currently, credit card payments cannot be accepted in person or through telephone banking.

4. Industrial Products sector - In January, The Fritzmeier Group, a producer of plastic assembly in Germany, metalworking, and environmental technologies, suffered a

cyberattack [109]. The provider has let its clients know that everything is still in emergency mode by posting a notice on the webpage. The number of businesses that have been assaulted is growing. The Fritzmeier Group, a producer of whole cabins, plastic assembly, metallurgy, and environmental technologies, was also harmed a few days ago. The has various sites in Germany and employs 2.200 people globally. The business is still running in emergency mode. Similar to other affected firms, communication appears to be either fully paralyzed or just partially functional. The likelihood that ransomware affected the business is quite high. But it's still unclear which one. The Fritzmeier Group is not yet included on the leak sites of LockBit, ViceSociety, Cuba, ALPHV, or BlackCat.

5. Chain Restaurant sector - In January, Yum! Brands, the parent organisation of KFC and Pizza Hut, was forced to close approximately 300 outlets in the UK following a ransomware attack [144] by an as-yet unspecified group. The US-based restaurant operator said that on detecting the incident, it implemented planned response protocols and deployed containment measures to prevent the malware from spreading. The Yum! Brands incident joins a growing list of ransomware victims so far in 2023. Some of the more high-profile UK victims have included Royal Mail, which is recovering its international export services following a suspected LockBit attack.

6. Consumer Staple Products sector - In January, Nuxe a French cosmetics brand, admitted to having suffered a computer attack and some of its software, but the rapid mobilization of its teams allowed it to restore its availability as soon as possible. On their official blog, which is hosted on the Darkweb, the Lockbit 3.0 ransomware group claimed responsibility for a cyberattack against the French cosmetics company. To remove or purchase the private data they allegedly stole from Nuxe labs, they demand $350,000 in cryptocurrency.

7. Steel Industry sector - In February, Vesuvius, a UK-based company specializing in molten metal flow engineering, published a warning to the public that it was handling a cyber incident [179] involving unauthorized access to networks. The ceramics manufacturer, which is listed on the London Stock Exchange, made no mention of the incident's nature and scope, the systems it damaged, or the identity

of the attacker.

8. Financial sector - In February, ION Trading UK was the target of a ransomware attack [145] that could take days to resolve, preventing dozens of exchanges from processing derivatives transactions. Reuters was told by the FBI that it was also aware of the attack but chose not to comment further. The incident caused the US Commodity Futures Trading Commission to postpone its weekly Commitments of Traders report. CFTC reports provide an overview of investors' positions in different assets. The Lockbit Group of attackers will release stolen data this February if the ION Group does not pay the demanded ransom.

9. Semiconductors sector - In February, a ransomware attack [50] on MKS Instruments Inc, a US public company, affected systems used in the manufacture of semiconductor equipment. As part of its containment efforts, MKS declared it would temporarily halt operations at some of its facilities. MKS Instruments is a supplier of subsystems for printed circuit boards, wafer-level packaging, package substrate, and semiconductor manufacturing with headquarters in Andover, Massachusetts.

10. Telecommunications Services sector - In February, LG Uplus, South Korea's third-largest wireless operator, apologized for recent leaks of its customer's personal information and internet service outages caused by DDoS attacks [98]. According to CEO Hwang Hyeon-sik, the reason the company took so long to respond was that it had to assess the situation first. As a result, it concentrated on defending itself from the attacks. At least 290 000 subscribers' personal information was stolen during the company's hacker attack in January. On January 2, the company discovered the leak, but it took them a week to inform the affected customers. Between January 29 and February 4, as a result of the cyber security breach, LG Uplus experienced a total of five DDoS attacks, which disrupted its internet service.

Over 70% of all ransomware activity in 2022 was targeted at manufacturing, with ransomware attacks on organizations that support industrial infrastructure nearly doubling. There is an increased risk for OT (operational technology) networks as a result of the fact that hackers continue to target numerous manufacturing sectors and subsectors. Only

39 of the 57 ransomware groups that target industrial infrastructures and organizations that Dragos monitored and analyzed were active in 2022, according to their research. An increase of 87% from the previous year brought 605 ransomware attacks against industrial organizations into 2022. Political unrest, the release of Lockbit Builder, and the continued expansion of ransomware-as-a-service (RaaS) are all factors that have contributed to an increase in ransomware activity [149].

3.4 Cyber Threats for Industry 4.0

The attacks mentioned previously are just a few concrete examples that occurred throughout 2021. It is essential to carefully analyze what is at the origin of these events, their possible consequences, for the safety of people, assets, and the impact on the normal functioning of organizations. Digital transformation brings new challenges and threats [157] to the security of industries, regardless of the sector of activity, as we saw in the attacks analyzed. The attacks mentioned above are only a few specific instances that occurred between 2021 and the first two months of 2023. It is essential to carefully analyze what is at the origin of these events, their possible consequences, for the safety of people, assets, and the impact on the normal functioning of organizations. Digital transformation brings new challenges and threats[70] to the security of industries, regardless of the sector of activity, as we saw in the attacks analyzed. Listed below are some of the online threats that industrial organizations are potentially most exposed to:

- The Nation-State Attacks - In the current global context, the exponential growth of online communication and interaction facilitates activities against other States. They intend to obtain competitive advantages in several domains, or the strategic sabotage of the targets' critical resources or infrastructure. Some groups of cyber attackers sometimes act under the auspices of a nation-state [107] to obtain credentials from employees of critical organizations or infrastructure, using, for example, different types of phishing [16]. They seek to identify weaknesses in the online security of their targets, for example, by exploiting known vulnerabilities, among other types of attacks. The targets can be systems [33]: nuclear power plants, energy distribution infrastructure and water resources, the pharmaceutical industry, military installations, etc.

- Intellectual Property (IP) Theft - The IP assets of any industry today, with all their IT and OT technology connected, are at serious risk of exposing attacks aimed at theft and cyber espionage on trade secrets [85], as happened with the development of vaccines for Covid-19. The targets of this type of attack were the scientists responsible and their teams for the research and development of vaccines for COVID-19 promoted by pharmaceutical companies [58]. Supply Chain Attacks - This is a strategy that is developed by compromising a supplier, or partner, which does not have a very consistent cybersecurity policy [30]. It is the starting point for executing a cyber attack on a large organization, which is the main target to hit. One method used, for example, is the theft of credentials obtained by installing a keylogger using social engineering [58] to gain unauthorized access to a workstation, with a false argument of technical assistance.

- Equipment Sabotage - The introduction of cheap microcontrollers in manufacturing hardware can become a risk factor in terms of quality assurance in general performance, also with the potential cybersecurity threats that may arise from their integration into production equipment [23], which can be, interconnected globally. Cybersecurity threats, in this context, can result from the exploitation of known hardware or software flaws, committed by internal or external attackers to organizations that are victims of sabotage [164].

- Phishing Attacks - An attacker contacts potential victims via an email or phone call from a trusted entity to impose a sense of urgency or intimidation on a superior. In this strategy, of social engineering, the intention is to put pressure on potential victims emotionally so that they make ill-considered decisions in carrying out actions. It is intended to influence the behaviour of those targeted, for example, by clicking on a malicious link sent via email from a supposedly trustworthy person or entity [17], to facilitate the theft of login credentials, credit card numbers, etc.

- Ransomware - It is malware that encrypts critical data of a victim system through a cyber attack, usually carried out by a group of attackers who intend to obtain a ransom in cryptocurrencies to ensure their anonymity [122]. Encrypted data requires a key that will supposedly be provided after the ransom is paid. There is also the possibility of a double ransom, in addition to the cryptographic key to decrypt critical data, attackers sometimes threaten to publish sensitive data stolen during the attack [131]. Attackers that execute ransomware frequently employ social engineering strategies, such as phishing, to enter a victim's surroundings. Also, keep in mind that you're working with cybercriminals, who occasionally fail to uphold their half of the bargain. The most typical varieties include [3]:

  - Crypto Ransomware or Encryptors - They make all encrypted content inaccessible without a decryption key, crypters are a more well-known and harmful variant.
  - Lockers - Completely block a system, restricting access to apps and files. The ransom demand is displayed on a lock screen, sometimes with a countdown to increase the sense of urgency and compel victims to respond.
  - Scareware - Fake software that tries to trick the user into thinking it has found a virus or another issue on his computer in order to persuade him to pay to have it fixed. While some types of scareware lock up your computer, others flood your screen with pop-up notifications without doing any harm.
  - Doxware or Leakware - Sensitive personal or business information could be published online via leakware, which causes many people to fear and pay the ransom to keep their private information safe.
  - RaaS (Ransomware as a Service) - The term "Ransomware as a Service" (RaaS) refers to a service that manages all parts of an attack, including the distribution of ransomware and payment collection.

- Advanced Persistent Threat (APT) - This is a continuous, sophisticated cyberattack planned in several stages, with a very well-defined purpose for data theft or sabotage, which can develop over a long time [55]. This type of attack is not only against large organizations but also their partners, whether small or medium, as a less protected access point until they reach the predetermined target [83][84]. APTs must be prevented, detected, and resolved by understanding their characteristics. Cyber espionage, theft of intellectual property or state secrets, criminal activity committed for financial gain, hacktivism, and destruction are the four main categories of APTs. APTs extract data from the network, which is most frequently done by stealing data, and then steal it. The typical APT life cycle involves infiltrating and attacking a network [187]:

  - Stage 1 Infiltration: In the first phase, advanced persistent threats often gain access through social engineering techniques. One indication of an APT is a phishing email that selectively targets high-level individuals like senior executives or technology leaders, often using information obtained from other team members that have already been compromised. Email attacks that target specific individuals are called "spear-phishing."
  - Stage 2 Escalation and Lateral Movement: Attackers can also create a "backdoor" that enables them to enter the network later and carry out covert operations. Attackers migrate laterally after gaining initial access to map the network and collect credentials, such as account names and passwords. In order to ensure that the assault can still proceed if compromised points are found and closed, other entry points are typically established.
  - Stage 3: Exfiltration: In a safe place on the network, thieves keep the stolen data without being noticed, they extract it or "exfiltrate." To shift the focus of the security team, they might employ strategies like a denial-of-service (DoS) attack. While the thieves are away, the network may still be compromised.

- Man-in-the-middle attacks (MITM) - are a common type of cybersecurity attack that allows attackers to eavesdrop on the communication between two targets. The attack takes place between two legitimately communicating hosts, allowing the attacker to "listen" to a conversation they should not be able to listen to. A conversation that should be private can be "overheard" by the attacker because the attack "sits" between two hosts that are actively communicating. The classic example of Eve managing to steal the conversation in plain sight gives Alice the impression that she is Bob and vice versa. The types of man-in-the-middle attacks are [106]:

  - Rogue Access Point - Attackers can set up their own wireless access points and manipulate network traffic, requiring physical proximity.
  - ARP Spoofing - ARP is used to resolve IP addresses to physical MAC (media access control) addresses in a local area network. When a host needs to talk to a host with a given IP address, it references the ARP cache to resolve the IP address to a MAC address. With some precisely placed packets, an attacker can sniff the private traffic between two hosts.
  - mDNS Spoofing - Multicast DNS is similar to DNS, but it's done on a local area network (LAN) using broadcasts like ARP. When an app needs to know the address of a certain device, such as tv.local, an attacker can easily respond to that request with fake data.
  - DNS Spoofing - ARP resolves IP addresses to MAC addresses on a LAN, and DNS resolves domain names to IP addresses. When using a DNS spoofing attack, the attacker attempts to introduce corrupt DNS cache information to a host in an attempt to access another host using their domain name. An attacker who has already spoofed an IP address could have a much easier time spoofing DNS.

3.5 Suspicious actions and methods to be monitored

Attacks come in several forms or methods, of which we are going to analyze some examples to awaken a critical analysis of this type of event. Although some of them are more complex and sophisticated, however, all of them are potentially a threat whether they are executed in an isolated way or integrated into a more elaborate strategy and oriented towards malicious purposes. Some types of attacks that should be considered relevant, to be neutralized in the planning and development of an IT/OT cybersecurity strategy stand out:

- Reconnaissance - For an attacker, it is a set of initial activities collecting system information to identify your security vulnerabilities and maliciously exploit them[62]. For a Pentester or a cybersecurity professional who performs intrusion testing, these activities are aimed at implementing corrective measures appropriate to these vulnerabilities and mitigating the risks of future attacks reinforcing the security of the system [82]. There are public, social and software reconnaissance activities, such as collecting public information on the internet and using phishing or social engineering techniques in contacting technical support to obtain restricted information. Or the use of specific software to perform ping scanning and port sniffing of packets.

- Social Engineering - An attacker through human interactions and assuming false identities attempts to psychologically induce the victim to breach security policies by revealing restricted access information [184]. Comparing a Malware attack with social engineering is more difficult to predict because it starts with a human error by a user with legitimate access to the system, who will be the target of an imminent attack.

- Malware - In essence, is malicious software, which in addition to the host can infect other network devices[84]. Used for espionage and data theft, and can maliciously alter the functioning of a system, among other threats [122]. It can be spread, for example, through malicious links or attachments in emails, which the user accesses, or performs as a routine action without the notion of the risks [58]. Malware is an element that integrates various types of attacks, such as Ransomware, Cross-Site Scripting (XSS), Trojan Horses, SQL injection, etc.

- Botnets - It is a network of devices infected with malware, as if they were remote-controlled robots, that will generate intentionally malicious traffic and coordinate for distributed and denial-of-service(DDoS) attacks, that is, invalidate incoming traffic to a certain server [122]. It can also be used for aggressive spam or click fraud campaigns. Here are some examples such as Mozi, Mirai, Cutwail, Coreflood, Ramnit, TDL4, etc.

- Web Application Attacks - An attacker can obtain a list of detected vulnerabilities using a web application scanner [193]. This type of tool allows auditing the security of online applications to identify vulnerabilities such as Cross-site scripting, SQL injection, Backup file check, Ajax testing, CRLF injection, SEL injection and XPath injection, etc.

- Phishing - This is a common tactic used by attackers who want you to install malware. In a phishing email, there must be a strong argument to convince you to take action. There will either be an attachment or a link in the email that needs to be clicked. You will infect your machine with malware if you open the malicious attachment.

- SQL Injection Attack - SQL is frequently used to manage data in server databases that hold essential data for websites and services. The attack works by exploiting any known flaws in the database, enabling the SQL server to run malicious code. by tricking the server into revealing information it wouldn't typically expose via malicious code.

- Cross-Site Scripting (XSS) - An attacker targets a vulnerable website to target its stored data in an attack resembling a SQL injection attack. However, a cross-site scripting attack may be chosen if the attacker would prefer to directly attack a website's visitors. When a user accesses the hacked website, the malicious code is only activated in their browser and targets them directly, not the website.

- Denial-of-Service (DoS) - The server of a website will get saturated if you overwhelm it with more visitors than it was designed to receive. Of course, there are innocent causes for this, but malevolent traffic overload happens a lot too. In some cases, multiple computers will carry out these denial-of-service attacks simultaneously. The term "distributed denial-of-service attack" (DDoS) refers to this kind of assault. Because the attacker can appear from numerous IP addresses all over the world, it can be much harder to defend against.

- Man-in-the-middle (MiTM) Attacks - Attacker can "listen" to communication that it normally shouldn't be able to hear because it occurs between two hosts that are actually communicating without knowledge that anyone else is doing so, ie without authorization to do so. The most common MiTM attacks are [106]:

  - Sniffing - An attacker may be able to view packets that were not meant for it to see, such as those directed to other hosts, if wireless devices are permitted to be used in monitoring or promiscuous modes. Attackers examine packets at a low level with the aid of packet capture tools.

  - Packet Injection - Malicious packets can be introduced by an attacker into data communication streams. Although harmful in nature, packets can appear to be a part of the conversation. In order to decide how and when to create and deliver packets, packet injection typically starts with sniffing. The monitoring mode on a device can also be used by an attacker to inject packets.
  - Session Hijacking - A temporary session token is created during login for the majority of web apps. The session token for a user can be found by scanning for sensitive traffic, and the attacker can then use it to send requests on the victim's behalf. Once the attacker obtains a session token and the user's password, he is no longer required to fake.
  - SSL Stripping - Attackers use SSL stripping to intercept packets and change HTTPS-based address queries to go to their corresponding HTTP endpoint, forcing the host to make requests to the server unprotected because employing HTTPS is a standard defence against ARP or DNS spoofing. Attackers can change HTTPS-based address requests to travel to their HTTP equivalent destination by intercepting packets and using SSL stripping. As a result, confidential information may be exposed in plain text.

- Session Hijacking and Man-in-the-Middle Attacks - The connection between the remote server and the requesting computer can be taken over by an attacker. An attacker may obtain the session ID and impersonate the machine submitting the request. As a result, they can intercept data travelling both ways, which is known as a man-in-the-middle attack. If everything goes according to plan, the web servers should then respond to your request by providing you with the data you requested.
- Credential Reuse - It's advised by security best practices to use different passwords for all of your websites and applications. Because so many people still use the same passwords, attackers rely on this fact. Whenever an attacker has a collection of usernames and passwords from a service or website that has been compromised, they are aware that there is a chance they will be able to log in if they use the same

credentials on other websites.

Chapter 4

Industry 4.0 - Regular assessment of threats and risks in short update cycles

4.1 Introduction

Cyber assaults were not viewed as a real concern in the industrial world for a very long time. Manufacturers are now employing more and more common industrial systems communication protocols. The International Society of Automation (ISA), International Organization for Standardization (ISO), and International Electrotechnical Commission are tasked with carrying out this function (IEC). A comprehensive strategy (workforce, organizational, and technological) that is in line with other security measures (information systems security and functional security), is practical from an economic standpoint, is long-lasting, and is customized to the unique data of a given business or facility is needed to establish a cybersecurity management system (CSMS) [100]. In Industry 4.0, the integration of processes and information in an IT and OT environment results from intensive use in different areas of its interconnected assets and tends to be online (ex.IIoT environments) [126]. A continuous reevaluation of risk management is imperative for organizations in the current cybersecurity context [24]. Security emerges as a permanent challenge that requires a preventive and systematic analytical approach in the development and implementation of effective policies, as well as in the monitoring of risks [169]. An attack on an OT network, on endpoints in industry 4.0, can be initiated through a set of actions to exploit vulnerabilities in the IT network [79]. The Internet of Things (IoT), Cloud Computing, and increasing automation are at the epicentre of Industry 4.0. which also contributes to increased exposure to online threats and cyberattacks [120]. Gradually, sophisticated cyberattacks are also targeting vulnerabilities that result from knowledge gaps due to a lack of convergence between IT and OT systems. And this is because, with the integration of new interfaces in IT and OT systems, there has been a significant growth of cyberattacks on ICS systems [41]. Not all nodes in a network are critical that is, they do not have the same importance in network connectivity. However, there is a need to identify the set of critical nodes whose performance, when compromised, can lead to maximum degradation of network connectivity, a problem known as the Critical Node Detection Problem (CNDP) [94]. With the introduction of new technologies and protocols in Industry 4.0, the challenge arises of minimizing a significant degradation of the control requirements to guarantee transparency in the connections and protection in different domains [7]. The transition in Industry 4.0. to the integration of IT and OT, and the processes of adoption of Industry technologies, is based on standards, reference architectures, and maturity models, among others. However, there is not one standardized framework but several for current processes and tools [32] with the aim, and complement, of adjusting to the technical perspective, and the organizational perspective, to provide a complete roadmap to guide the processes of integrating both in line with the constraints and specific needs of an organization [126].

4.2 The Challenges Of IT/OT Security

The increasing technological complexity [99] between IT networks and OT networks, and their complementarity, are constant challenges for Industry 4.0 [182]. IT covers the management of information systems, and OT covers the management of industrial operations.

In IT the most common security requirements priority is the CIA triad [91]: Information Confidentiality, Data Integrity and Systems Availability. IT manages transactional flows of data, voice and video, that is, large amounts of information. A failure in the IT network can lead to significant loss of sensitive data, compromise its integrity and confidentiality can also affect its availability [177] with unpredictable consequences for the business. For management and security reasons, access to the IT network requires the authentication of users and devices to access the organization's resources [181]. It is a constantly changing environment as a result of technological massification, with increasingly shorter cycles of adoption of new IT tools [78].

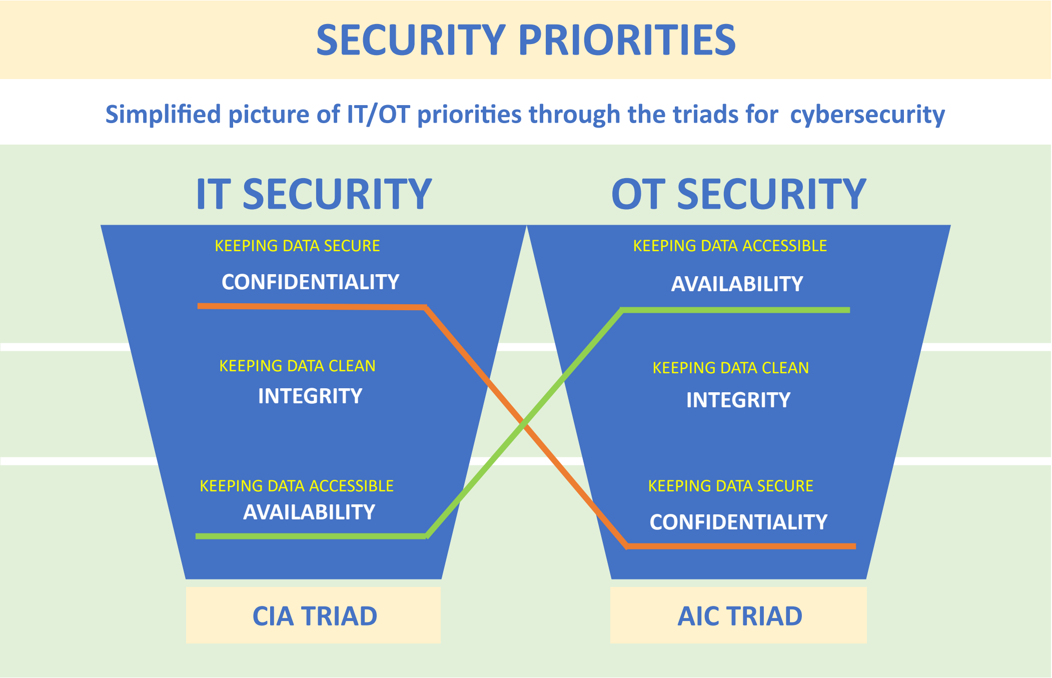

Figure 4.1: Cybersecurity: Simple view through triads of IT/OT priorities

In OT the most common security requirements priority is the AIC triad [91]: Availability of data flow and controls, Integrity of configuration data and Confidentiality of the flow of all types of data as well as those obtained by monitoring ICS/SCADA [18]. OT interacts with machines being more industry oriented, generates and processes real-time control, monitoring and supervision data [117]. OT networks are not always, configured for data protection levels in line with standards considered adequate for known [64]. It is also an environment with longer technology refresh cycles compared to IT, which does not always allow for more data to improve service quality and increase the efficiency of product lifecycle management [191]. OT networks control physical access to any device failures that can impact the life of devices and interfere with production processes [108]. Updates are implemented, in line with planned operational maintenance [197], given the nature of OT technologies and the dynamics of near-nonstop manufacturing [143]. Focusing on the essentials, we can summarize the differences between IT and OT as described above [180]:

- The most important factors in the IT industry are usually confidentiality, integrity, and availability. It is considerably more crucial that your secrets are always kept private and that no one is sending emails on your behalf or obtaining unauthorized access to critical papers on a computer or in transit. When you take into account that brief disruptions in IT systems seldom have an impact on the actual world, making sure all systems are available at all times becomes less crucial.
- In addition to privileged credentials and access, ”confidentiality” covers OT data such as process parameters and production rates. This might be the most significant CIA triad component in the context of OT. Illegal access to OT assets calls into question integrity and might jeopardize quality and safety protocols. Attacks on availability include the latest one on the Colonial Pipeline and the 2019 ransomware assault on the Springhill Memorial Hospital.
- Every organization has different needs when evaluating the CIA triad, and they should take the time to properly consider what is best for them. As cyber-attacks continue to expand on an international scale, efforts like this can make or break the future of an organization.

4.3 Nist Cybersecurity Framework - Best practices to manage cybersecurity risk

It is an essential framework because it allows understanding, managing and expressing cybersecurity risks through a common language [143] for all involved organizationally, both internally and externally. Industrial activity poses unique risks that result from industrial activity, such as different risk tolerances and types of vulnerabilities. Organizations should tailor and customize their checklist and avoid a single linear approach to their critical infrastructure because of the unique risks involved [123]. To effectively manage cybersecurity threats, it is important to understand the organizational business drivers and specific security concerns related to its use of technology. Many firms already have procedures in place for handling civil rights and privacy issues. Although the Framework is technology-neutral, it is nonetheless helpful and promotes technical innovation. It employs contemporary conventions and methods, which transform as technology develops. The Framework, which consists of three components—the Framework Core, the Framework Implementation Tiers, and the Framework Profiles—is a risk-based strategy to managing cybersecurity risk. Each element of the Framework strengthens the relationship between cybersecurity operations and business/mission drivers. There are three main components of the Cybersecurity Framework [165]:

- The Framework Implementation Levels describe how the organization manages cybersecurity and its main characteristics, for example, the recognition of risks and threats, or the way it decides on the various levels, such as Informed about the risk (Level two).
- The Framework Core contains informative references and structured activities focused on specific cybersecurity outcomes, and in terms of risks, it also allows communication between them the entire organization. It is organized into Functions such as Identify, Protect, Prevent, Respond, and Recover [165]. Added to this are Categories such as Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management. Also in Subcategories, compose an example: the subcategory “ID.BE” of the Category “Business Environment” of the “Identify” Function, that is, “Function - Identify - Business Environment - ID.BE”. And finally in Informative References such as for ID.BE-1: COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05; ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2; NIST SP 800-53 Rev. 4 CP-2, SA-12.
- The Framework Profiles allow for describing the current state of cybersecurity activities, or intended state, facilitating the alignment of the organization’s business requirements, risk tolerance and resources to roles, categories and subcategories [165]. Define a road map for cybersecurity risk reduction that reflects risk management priorities, industry best practices, and organizational and sectorial goals, among others considered essential by each organization, such as the NISTIR 8183 - Cybersecurity

Framework Manufacturing Profile. NISTIR 8183 can be used as a road map for manufacturers in line with the goals and best practices of the manufacturing industry to reduce cybersecurity risk [166].

4.4 Assess the Organization's Current Internal and External Threats

Industry 4.0 relies on data to run its operations and has exponentially increased the number of entry points exposed to cyber threats. With the attack surface widening for potential cyberattacks, reassessing threats is essential to identify whether they are internal or external, like in these two examples:

- Employee Negligence - Compromised confidential data can result in penalties with relevant economic consequences for organizations in response to the Covid-19 pandemic [12], which has shifted a part of their employees to remote work [72]. From lost storage devices to data accessed from insecure home systems [20] to malicious and disgruntled employees [160], to the usurpation of the identity [113] of other employees are all examples of how internal human behaviour can be a threat to take very seriously. But there are also situations of management errors, for example, according to IBM's Cost of a Data Breach Report 2021 [155], more than half of employees in remote work have not received new guidelines [71] on how to mitigate digital risks in handling your customers' personally identifiable information.
- Email Phishing - The results and indicators related to phishing emails reported [113] by employees can also constitute an imminent external threat. In this second example, the focus is on a possible pattern of threat from the outside. An employee's negligence can convert this external threat into an effective attack within the organization [22]. It is a potential threat in the spread of Malware, be it a Trojan or a backdoor, a trap ready to be unleashed for a sequence of events with unpredictable consequences. The most common type of cybercrime in 2021 [119], according to Statista, reported to the US Internet Crime Complaints Center, was phishing and similar scams, with approximately 324,000 individuals affected and close to 52,000

cases of personal data breaches during the same year.

In these two examples, a common element is a human factor exposed to risks that are revealed in part through published data 2021 [173]:

- Malicious URLs are 3-4 times more common than malicious attachments.
- More than 20 million messages contained malware associated with an eventual ransomware attack.
- The average phishing simulation failure rate was around 11% in Production Engineering, Operations and Project Management departments.

4.5 Vulnerabilities: The Importance Of Cwe, Cve And Owasp

During the software and hardware development process [66] [4], whether for IT or OT, weaknesses or anomalies are identified that are corrected or eliminated. Malicious people [47] can exploit weaknesses in a system to cause damage to an organization and its partners. The complexity of integrating, emerging IT/OT technologies [139] based on cyber-physical systems (CPSs), as well as digital tools in industry 4.0, requires regular monitoring to assess the possible risks of being exposed to cyber-attacks. Vulnerabilities in hardware and software can compromise operational assets, compromising the integrity of the pre-established processes [32] from an extensive list of hardware and software integrated throughout the entire value chain of manufacturing. Vulnerability identification is a step essential after mapping Industry 4.0 assets to prevent threats and attacks. In organizations, a cybersecurity team that is constantly alert and well-informed is essential in preventing and mitigating constant risks [120]. Organizations can use the CVSS Score to assess the most vulnerable points in their systems and plan security measures. After a query on 2022-08-15 to the online database CVEDetails [132], a total of 181965 vulnerabilities were obtained. Between 2012 and the date of this query the value was 133999 vulnerabilities. More data can be analyzed In Fig. 4.2 and Fig.4.3:

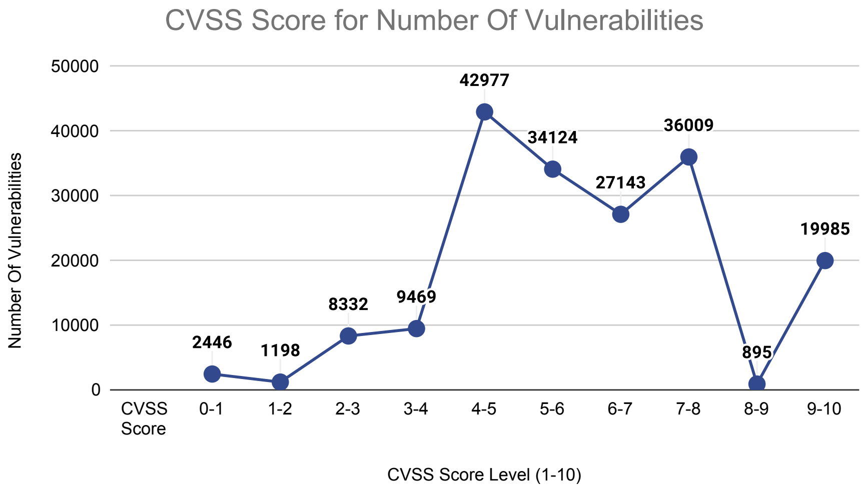

Figure 4.2: Distribution of all vulnerabilities by CVSS Scores - based on data collected on 2022/08/15

In Fig. 4.2 we can see the distribution, based on data collected on 2022-08-15, of all vulnerabilities by CVSS scores. The highest number of vulnerabilities is around 42977, with a CVSS Score between 4-5, a medium severity degree. The second highest value is about 36009 and is in the CVSS between 7-8 with a high degree of medium severity. At the top of the CVSS scale, which is between 9-10, we have about 19985 vulnerabilities recorded. It is worth noting that the CVSS Score range between 6-10 has a total of 84032 vulnerabilities corresponding to 46% of the total recorded in the database.

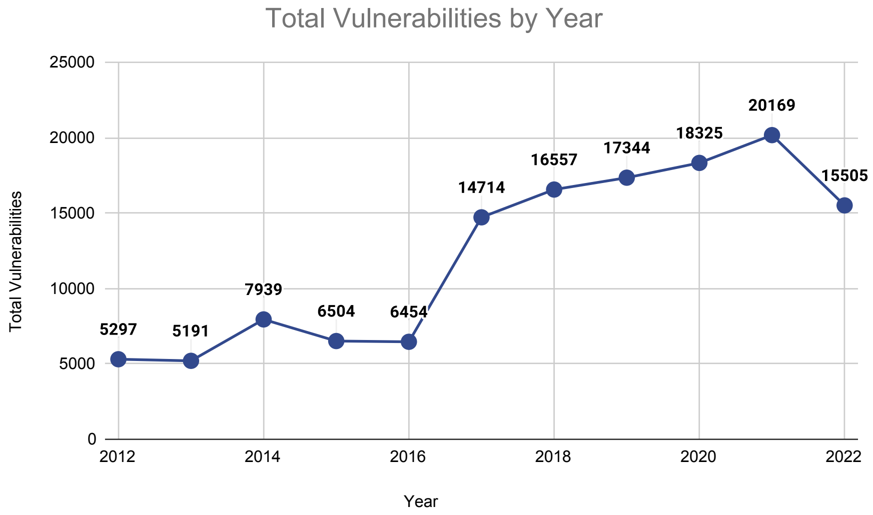

Figure 4.3: Total Vulnerabilities by Year from January 2012 to August 2022 - based on data collected on 2022/08/15

In Fig. 4.3 can see the growth of vulnerabilities from 5297 in 2012 to 20169 in 2021, the 2022 value of about 15505 is only up to August 15th. The highest growth occurred between 2016 with 6454 and 2017 with 14714, that is to say with around 8260 new vulnerabilities, an increase of 56.14%. From 2017 the growth was steady until 2021 with more than 20000 vulnerabilities. There are open online information sources that many cybersecurity professionals use as a reference, as described in the following three topics, to help them find potential vulnerabilities within the technological complexity of industry 4.0.

What are Common Weakness Enumeration(CWE)?

The CWE list [37] results from a community effort to identify the most common security weaknesses in software and hardware. It describes flaws, and different types of errors in the implementation of software or hardware, among others, that make them vulnerable to attacks. And above all, it is intended to be a starting point for a common language, for critical analysis of identified software and hardware vulnerabilities, and thus to develop strategies to mitigate and prevent attacks.

The CWE 4.8 version is intended to facilitate the research on weaknesses and their interdependencies and is organized mainly according to abstractions of behaviours such as:

- Organizes weaknesses around concepts that are often used or encountered in software development.
- Organizes weaknesses around key concepts that are often used or encountered in hardware design.
- Research Concepts make it easy to research weakness types and organize items by behaviour using various levels of abstraction.

What are Common Weakness Enumerations (CWE)?

The CVE is a public list [35] of currently identified security flaws of a specific instance of a system/product, ie related to specific systems and products. A vulnerability is a weakness or a flaw that can be exploited maliciously and could negatively impact the confidentiality, integrity or availability of one or more components of any system.

Through the work of the CVEProgram, we can standardize the identification of a vulner-

KEYWORDS	TOTAL	2022	2021
LoRa Protocol	3380	236	448
API	3329	290	590
Smart Meter	1358	41	113
Cloud	1240	85	223
Gateway	1208	55	103
IoT	1069	23	248
Embedded	935	14	76
Industrial IoT (IIoT)	878	14	216
Bluetooth	583	62	93
TCP/IP	343	12	34

Table 4.1: Some examples of the most common technologies in industrial environments and their registered vulnerabilities.

KEYWORDS	TOTAL	2022	2021
Denial of service	29573	891	2100
Injection	15260	1306	1457
SQL injection	10306	864	629
MYSQL	1658	141	204
Cryptographic Failures	701	141	204
LDAP	648	45	44
SSRF	615	97	129
HTTP Session	350	25	37
TensorFlow	323	80	204
Broken Access Control	62	12	19

Table 4.2: Some examples of the most common technologies in information technology environments and their registered vulnerabilities.

ability which allows us to establish the correlation of vulnerability data between systems, among others.

Next, some examples are presented, in table 4.1, which, although not all of them are exclusive to OT environments, reveal some of the complexity of the convergence of technological problems with the IT environment that we can observe in table 4.2.

The numbers of vulnerabilities are also represented from the total records since 1999, as from the years 2022 and 2021. These are obtained using the Search CVE List online tool.

Category	CWE
A01:2021-Broken Access Control	1345
A02:2021-Cryptographic Failures	1346
A03:2021-Injection	1347
A04:2021-Insecure Design	1348
A05:2021-Security Misconfiguration	1349
A06:2021-Vulnerable and Outdated Components	1352
A07:2021-Identification Authentication Failures	1353
A08:2021-Software and Data Integrity Failures	1354
A09:2021-Security Logging Monitoring Failures	1355
A10:2021-Server-Side Request Forgery (SSRF)	1356

Table 4.3: Weaknesses in OWASP Top Ten (2021).

What are Open Web Application Security Project (OWASP)?

One of its principles is the sharing of knowledge on how to improve the security of web applications [129]. This knowledge sharing through forums, networking, training tools and resources, and specific documentation.

A good example is the OWASP Top 10 document fundamental is standard security awareness for web application developer communities, recognized as the first step towards more secure coding. This document brings together the most critical security risks for web applications. The list of top ten risks for web applications in 2021 is in Table 4.3 [130].

CPSs can also have significant privacy consequences that are not anticipated, by new system designers, in addition to security and protection-related issues. Similar cultural assumptions around privacy are being challenged by the development of CPS technologies in general and consumer IoT in particular. These devices have unprecedented levels of granularity for collecting physical data from many human activities, such as electricity use, location data, driving behaviours, and biosensor data.

People are usually unaware of how much personal information is acquired on them due to the passive way it is done. Because information gathered by companies, can be obtained by other actors through means with questionable legality, this data collecting exposes them to the prospect of being targets for spying or illegal activity.

Some car manufacturers are known to collect information about speed, internal and external temperature, battery life and range. In practice, they are remotely collecting a variety of data from the cars' driving history [147].

4.6 Guidelines And Standards To Cybersecurity Frameworks

A cybersecurity audit is a systematic examination of the activities carried out to verify if they comply with the most demanding standards recognized by the market as references of excellence in security [48]. The company must provide written proof of the policies put in place in accordance with the requirements of the certification it seeks. Here are some examples of cybersecurity policies and standards that can be adopted:

- Cybersecurity Capability Maturity Model (CMMC) [19] - Emerged in the USA as a need to correct the low compliance rates across the Defense Industrial Base (DIB) associated with NIST SP 800-171[35] and as a mandatory prerequisite for companies, from various areas, with CMMC certification can bid in tenders to formalize government contracts.

- FedRAMP Federal Risk and Authorization Management Program - It is a standardized approach [10] that results from the collaboration between various government agencies, such as NIST, GSA, DoD, and DHS, allowing the federal government to adopt secure cloud services offered by cloud providers. Its focus is infrastructure and cloud applications. The technical details are guided by the publication NIST 800-53 [40] about Security and Privacy Controls for Federal Information Systems and Organizations.

- ISA IEC 62443 Industrial Cybersecurity Standards - Developed by the ISA99 committee [75] which is made up of cybersecurity experts from different countries, with a mission to develop consensus standards for all sectors of industry and critical infrastructure [68]. They produced the ISA/IEC 62443 series of standards is a flexible framework to address and mitigate current and future security vulnerabilities in Industrial Automation and Control Systems (IACS).

- ISO/IEC 27000:2018 information security management system (ISMS) - Provides overview, terms and definitions of information security management systems (ISMS) [76], which apply to every type and size of the organization. It is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes. It protects information assets and facilitates management, measurement and continuous improvement. It guides the approach to the three dimensions of information security: Confidentiality, Integrity and Availability.

- ISO/IEC 27036-1:2021 Cybersecurity Supplier relationships - This document [77] addresses the perspectives of acquirers and suppliers, giving detailed implementation guidance, for the protection of their information and information systems, on the controls that deal with these types of relationships and which are described as general recommendations in ISO/IEC 27002.

- NIST 800 82r3 Guide to Operational Technology (OT) Security - The document provides an overview of OT and system topologies [167], as well as guidance on how to secure different types of control, automation, monitoring and industry systems. It also identifies typical threats and vulnerabilities and provides recommended security countermeasures to mitigate associated risks.

- NIST 800-207 Zero Trust Architecture - In the corporate context, it is still necessary to deal with the challenges of “obsolete” networks in the current context of cybersecurity, and also with the new paradigm of remote work, the document presents a systematic set of guidelines to improve the cybersecurity of companies. This document presents an abstract definition and describes the main structural logical components of a zero trust architecture (ZTA) [151][134]. It is oriented not towards network segments but towards constraining small groups of resources at the expense of large perimeters, in line with corporate trends towards cloud-based assets and remote work. It also presents general deployment models.

- NIST 1800-10 Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector - In this guide [138], the architecture and solutions presented are some of the commercial standards-based products that implement standard cybersecurity features such as behavioural anomaly detection (BAD), application whitelisting (AAL), file integrity checking, management change control and user authentication and authorization. The guide also contains information to guide three types of professionals: NIST SP 1800-10A for business decision makers, NIST SP 1800-10B for technology, security/privacy program managers, and NIST SP 1800-10C for professionals of technology.

- NIST 800-181 revision 1: The Workforce Framework for Cybersecurity (NICE Framework) - It is a framework that guides the simplification of communications, the sharing of information and a focus on the cybersecurity work to be performed. Guides to improve communication on how to identify, recruit, develop and retain cybersecurity talent [135].

- SOC 2 [156] is a voluntary compliance standard that specifies how service organizations should manage customer data, developed by the American Institute of CPAs (AICPA). A SOC 2 report is tailored to the unique needs of each organization, informing its partners on how it manages its data, and there are two types of report: type 1 describes the organization's systems and whether the system design complies with the principles of relevant confidence and type 2 where the operational efficiency of the systems is detailed.

4.7 MITRE ATT&CK - Knowledge base for cybersecurity

MITRE ATT&CK is commonly used to describe and classify how malicious actors conduct reconnaissance, initial access, persistence, lateral movement, exfiltration, and many other tactics. Malicious events are categorized by one or more specific techniques which are grouped into high-level tactics. All the techniques are grouped by tactics and can be identified by their IDs [93][138]. A knowledge base for cybersecurity experts interested in developing safe systems, programs, and services is called MITRE ATTCK® and is available online and to the general public. Based on the requirement to document advanced persistent threats against corporate networks using Windows-based solutions, MITRE launched the FMX project in 2013, which was aimed at enhancing post-compromise detection of adversaries in corporate networks. We can find 3 groups of tactics that are designated Enterprise, Mobile and ICS [170]:

- Enterprise tactics - Contain subgroups such as Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact and Mobile.

- Mobile tactics - Contain subgroups such as Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact.
- ICS tactics - Contain subgroups such as Initial Access, Execution, Persistence, Privilege Escalation, Evasion, Discovery, Lateral Movement Collection, Command and Control, Inhibit Response Function, Impair Process Control and Impact.

The MITRE ATT&CK Matrix

Contains a set of techniques used by adversaries to accomplish a specific objective. The objectives are presented linearly from the point of reconnaissance to the final goal of exfiltration or "impact". Those objectives are categorized as tactics in the ATT&CK Matrix. Adversary techniques, which outline the actual actions the adversary takes, are included in each tactic of the MITRE ATT&CK matrix. Some techniques have subtechniques that go into greater detail about how an enemy employs a particular technique. And there are more four concepts to highlight [168]:

- Tactics - It's the objective, the reason, and the intention of an attack Techniques - It is how an action is materialized, an attack with a tactical objective.
- Sub-Techniques - Categorize behaviour one level lower than a technique, being even more specific in detail
- Procedures - These are a set of specific implementations of techniques and subtechniques, such as a procedure that contains a mix of PowerShell, Process Injection and Credential Dumping sub-techniques in relation to LSASS behaviours.

4.8 Zero Trust Security: Simplifying Cyber Compliance

Zero Trust emerges as a strategic cybersecurity approach to validate all the essential steps of digital interactions, which denies the principle of implicit trust to reinforce security in a way appropriate to the needs and context of the organization [152]. With the evolution of different technological paradigms, such as cloud assets, policies that allow users to access data through their equipment (BYOD) [9] and remote work, cybersecurity, instead of the circumscribed perimeters owned by organizations, increasingly focuses on three vectors: assets, resources and users. The traditional concept of an organization's network perimeter is expanding, whether through remote work, with BYOD or the migration of data and applications to the infrastructure of cloud service providers, such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud, IBM Cloud, Oracle, SAP, etc. The Internet of Things (IoT), a growing collection of connected devices, has a wide range of security flaws. IoT device security is essential because current IoT devices have the potential to harm people by interacting with the physical world. It could be argued that every time a business releases a product as a component of a global ecosystem, they have a duty to offer security updates.

The IoT benefits from connectivity that facilitates collaboration among a variety of computing systems, ranging from sensor nodes and mobile devices to large control systems and cloud computers. The consequences from attacks on the IoT can be more devastating than information theft or financial loss. Here, we propose locally centralized, globally distributed authentication and authorization for the IoT to address these problems. The lack of adequate access control methods contributed to the linked devices' incapability to withstand exposure to the wild. Things that weren't previously connected to the Internet, a hostile landscape, are now doing so. The process of deciding whether a device or user has access to resources, such as the ability to read or write data, run programs, or control actuators, is known as access control, sometimes known as authorisation [86].

Zero Trust is a set of principles based on the NIST SP 800-207 document, which contains a set of cybersecurity guidelines that provide federal agencies with detailed recommendations on how to keep and protect data privacy. The principles are oriented so that all authentication and authorization of resources are dynamic and applied effectively before access is allowed. In the 2022 "NIST CSWP 20 - Planning for a Zero Trust Architecture" document, they are organized as follows [151]:

- Network Identity Governance: Access is only allowed after resource authentication and authorization.

- Endpoints: Computing resources are all data and services, which the company monitors and measure the integrity whether of the resources themselves or associated.
- Data Flows: Access to resources is determined by dynamic policies and per session to individual enterprise resources. Much information as possible is collected, by the organization itself, about the current state of assets, network infrastructure and communications to reinforce cybersecurity.

Chapter 5

Industry 4.0 and the Smart Grids: Sustainability, Interoperability and Cybersecurity

5.1 Introduction

Industry 4.0, which is made possible by the use IoT, cloud computing, machine learning, and CPS, covers the entire life cycle of the product, from production to supplier to end user. Smart Grids uses information and communications technologies to enable the fourth stage of the industry. Energy for the smart factory is provided by Smart Grids between components of various systems, and machine learning can use data to make complex decisions [141].

Modernisation of the world's electric grids is needed to take advantage of new technologies, such as integrating renewable sources of energy, deploying smart meters and exchanging electricity between consumers and the grid [147].

A nation's essential infrastructures are supported by its cyber system. In order to safeguard both national security and economic growth, they must operate reliably and securely. A nation's essential infrastructure is supported by its cyber system, which must operate reliably and securely to safeguard national security and economic growth. Severe effects on the reliability and security of physical systems that rely on a cyber system can result from a serious security event. Cyberattacks on vital infrastructure systems, such as power grids, are becoming more frequent and sophisticated [171].

5.2 Sustainability with Smart Grid

The conventional power system made it challenging to keep track of energy use, which resulted in an overuse of electricity and the production of harmful greenhouse gas emissions from the burning of fossil fuels. This resulted in excessive pollution, detrimental health effects, and disproportionately harmful effects on environmental justice communities. Sustainability materialises when consumers are allowed to minimise their environmental impact by using less energy thanks to the smart grid. By consuming energy only when needed and eliminating waste, smart meters and thermostats can help make homes and buildings more energy efficient [31].

Renewable energy sources are being rebalanced to meet environmental and other issues since there is a connection between energy and environmental concerns. In order to reduce greenhouse gas emissions, which are the primary cause of climate change and ecological effects, low-carbon power generation is being given priority. Unless there is a considerable change in how existing electric grids are administered, the International Energy Agency has assessed that present power networks would assure that global temperature rise exceeds the targets of the Paris Accord. To do this, power systems must abandon century-old traditions and concentrate on incorporating dispersed technology and sustainable energy into their systems. Coordination across the electrical system is needed to account for things like demand fluctuations that are caused by nature, some renewable resources, operational uncertainty that develops as dispersed technologies move control methods to the edge of the system, and other considerations [60].

Through the use of resilience roadmaps, sensors, high-definition cameras, and real-time situational awareness, power utilities should develop a forward-looking strategy for resilience against future hazards, such as wildfires, extreme weather events, and cybersecurity risks. By using fewer raw materials, adopting sustainable materials, putting circular solutions into practice, and safeguarding biodiversity, the United Nations Sustainable Development Goals should be achieved. Can lessen the environmental impact of the life cycle and improve safety, especially as critical mineral resources become scarce. The rollout of smart meters and the automation of substations, feeders, lines, and transformers through the use of sensors and monitoring tools are both initiatives of the distribution sector, which is also the largest investor in digital infrastructure. Digital investments also cover non-wire alternatives like flexibility services, distributed standalone storage systems, and network digital twins. The digitalization of power transformers, automation of substations, creation of flexible alternating-current transmission systems (FACTS), and development of cutting-edge sensors are the focus of digital investment in the transmission industry. Despite increasing by more than 20% in 2021, public charging infrastructure for electric vehicles still account for less than 5% of distribution investment [161].

5.3 Interoperability with Smart Grids

The Smart Grid is a transmission network that effectively overlays the Internet on the grid by fusing cutting-edge power engineering with cutting-edge detection and monitoring technology. The transmission grid will be very different from the current grid due to these technological developments, using less energy because it can quickly address problems like traffic jams and other interruptions, which lowers energy loss. It can also link new generators to the transmission grid, facilitating a greater integration of renewable energy sources [61].

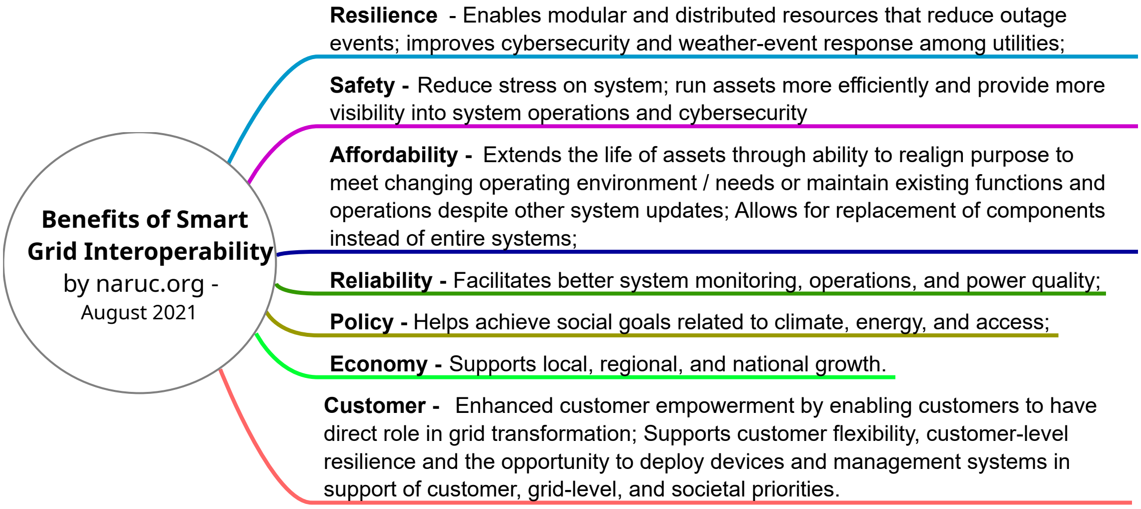
Benefits of Smart Grid Interoperability
by naruc.org -
August 2021
Resilience - Enables modular and distributed resources that reduce outage events; improves cybersecurity and weather-event response among utilities;
Safety - Reduce stress on system; run assets more efficiently and provide more visibility into system operations and cybersecurity
Affordability - Extends the life of assets through ability to realign purpose to meet changing operating environment / needs or maintain existing functions and operations despite other system updates; Allows for replacement of components instead of entire systems;
Reliability - Facilitates better system monitoring, operations, and power quality;
Policy - Helps achieve social goals related to climate, energy, and access;
Economy - Supports local, regional, and national growth.
Customer - Enhanced customer empowerment by enabling customers to have direct role in grid transformation; Supports customer flexibility, customer-level resilience and the opportunity to deploy devices and management systems in support of customer, grid-level, and societal priorities.

Figure 5.1: The benefits of interoperability span technical, economic, political and social systems

Operating a modern grid will require a diverse portfolio of energy resources and multiple economic structures, according to the National Institute of Standards and Technology (NIST), which noted that the power grid is changing. Modular and distributed resources are enabled by resiliency, which also improves cybersecurity and the ability to respond to weather-related events, decreases system stress, maximizes resource usage, and increases asset longevity. The benefits of interoperability span technical, economic, political and social systems and can be conceptually understood using the seven categories as a framework, described in Figure 5.1 [59].

The power system's interoperability is a crucial but underdeveloped capability that has been hampered by the development of new technologies and related standards. The NIST Smart Grid Interoperability Framework describes a new set of interoperability perspectives using developing technology and power system architectures. It protects against technological obsolescence, increases the return on equipment purchases, and promotes combinatorial innovation. Traditional security procedures must be taken into account to ensure interoperability. The advantages of an interoperable smart grid for the environment are best understood in this context [60]:

- The advantages of an interoperable smart grid for the environment are best understood in this context - Improved utility-scale use of sustainable energy technologies: Renewable energy resources are more variable than conventional resources, and utilities must now manage against relatively large-scale contingencies. An interoperable smart grid is needed to improve system flexibility and maximize the potential for displaced high-polluting resources.

- Combining customer-sited resources' environmental advantages: Most of the energy required to create electricity is lost physically during power generation, transmission, and distribution, which means that very little of it ever reaches the consumer. As a result, more power generated near the customer's location may be put to better use than electricity generated at more remote sites. To minimize upstream greenhouse gas emissions using effective energy resources, interoperability is essential.

- Putting off infrastructural improvements: Since peak demand is rarely met, electrical grids are built to handle it, reflecting a design philosophy that significantly underutilizes system capacity. To address this, an interoperable smart grid can affordably defer or replace capacity upgrades with wireless alternatives, coordinated energy efficiency and DER deployments. Estimated capital savings from postponing infrastructure upgrades total $10 billion annually; these funds could be used to support more significant long-term emissions reductions and clean energy targets.

- Connected infrastructures' decarbonization: To meet sustainability goals, it is necessary to electrify energy infrastructures in the building, industrial, and transportation sectors using an interoperable smart grid. This would make it possible for previously independent systems and actors to depend on one another and exchange information, as well as make it possible to integrate various resources and technologies.

5.4 Cyberattacks on Smart Grids

Smart Grids are managed by highly developed computing, control, and networking infrastructure; however, cyberattacks are on the rise as a result of both internal and external vulnerabilities. They have an effect on the whole smart grid ecosystem. It also examines the weaknesses of each smart grid component, including the operating system, hardware, software, data management, data communication, services, and complex smart grids [42].

A smart grid is a generation of electrical power systems that aspire to achieve reliability, flexibility and efficiency with environmentally friendly operation. More energy is being produced globally using renewable energy sources. The usage of renewable energy sources has grown substantially in order to create more energy globally, and the digital communication network—which depends on a shared real-time information system—is the most important part of smart electric grids to be safeguarded from cyber criminals [153].

Demand-response programs provide incentives to reduce electricity consumption during peak hours, preventing load-altering attacks and improving power grid stability and energy efficiency. Incentives from the utility or demand-response provider are the basis for the programs that are used by large commercial consumers and government organisations to manage large campuses and buildings. The attack surface for load-altering attacks is expanding as these programs gain more traction and can control a load of their customers from a distance. An attacker can gain access to the enterprise by controlling remote loads and changing a large amount of load to affect the power system, cause system inefficiencies, gain economic advantage, or cause load changes sufficient to change the frequency of the power grid and cause blackouts on a big scale. Counterattacks on electrical networks can cause frequency instabilities, line failures and increased operating costs. Creating a system blackout or a blackout of a large percentage of the bulk power grid can be difficult due to the lack of protections for load changes, including under-frequency load shedding [50]. Security for the smart grid must be prioritized in order to deal with serious security problems like intentional attacks, user error, equipment failure, and natural disasters [38].

Systems used in smart grids are impactful and dangerous because they are cyber-physical and susceptible to cyber-attacks. The attackers target different layers of systems architecture and aim to interfere with the security of different types of devices: sensors, network devices, and smart meters, among others. Some examples of threats to the grid's security are [141]:

- DoS attacks are difficult to detect and difficult to block, so cyber-resilient systems are needed to reduce their impact.
- Data injection attacks can have strong negative impacts on power systems, so it's critical to use smart security systems with dedicated authentication to stop them.
- In smart grids, users' privacy must be protected because information about their location, payments, power use, and preferences can be used maliciously to track and harm them. anonymisation, source masking, encryption, and data aggregation are privacy-preserving techniques.
- Insider threats can be avoided through hiring procedures, background checks, and technological tools like anomaly detection systems and authenticated access control.

The Internet of Things is a network of connected devices that can wirelessly exchange data with one another. These IoT nodes may include a microcontroller unit (MCU), gateways, firmware, local memory, wireless connectivity, cloud platforms, sensors, and I/O connections. The network nodes may be housed in a single device, a module, or a group of devices. Innovations in system-on-chip (SoC) technology have made it possible to integrate a growing number of functions onto a SoC or into a system-on-module (SoM). Depending on the applications, communication protocols and common IoT application protocols used for messaging can be one or more of the following [90]:

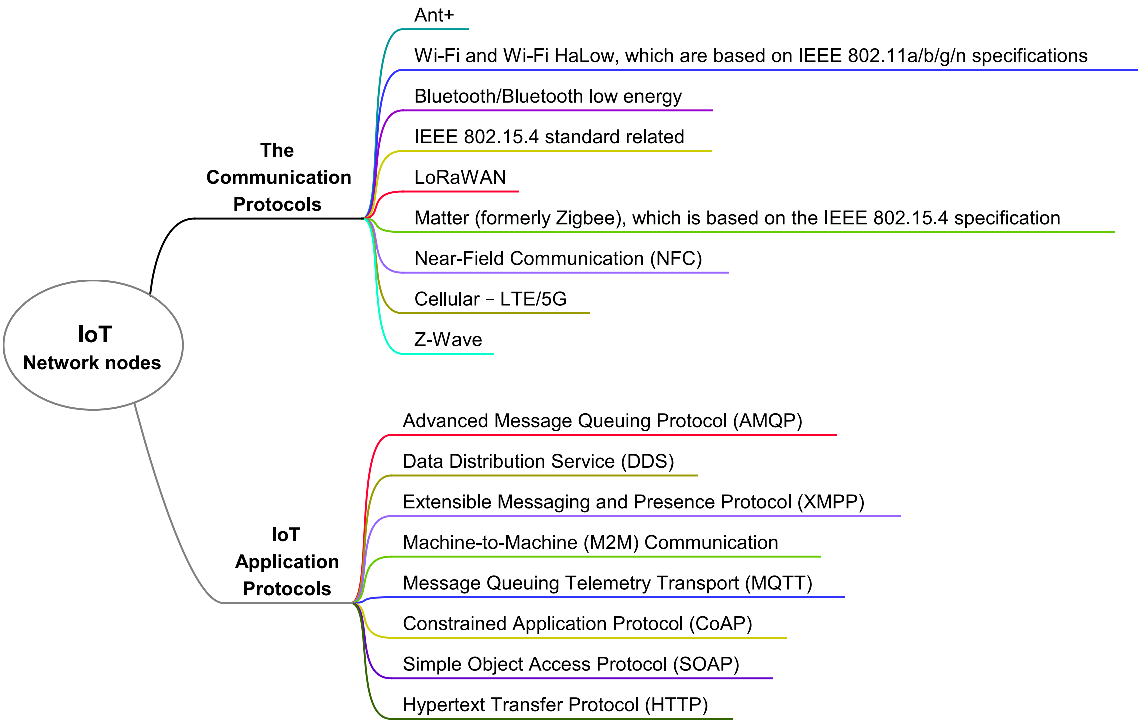
IoT
Network nodes
The Communication Protocols
Ant+
Wi-Fi and Wi-Fi HaLow, which are based on IEEE 802.11a/b/g/n specifications
Bluetooth/Bluetooth low energy
IEEE 802.15.4 standard related
LoRaWAN
Matter (formerly Zigbee), which is based on the IEEE 802.15.4 specification
Near-Field Communication (NFC)
Cellular - LTE/5G
Z-Wave
IoT Application Protocols
Advanced Message Queuing Protocol (AMQP)
Data Distribution Service (DDS)
Extensible Messaging and Presence Protocol (XMPP)
Machine-to-Machine (M2M) Communication
Message Queuing Telemetry Transport (MQTT)
Constrained Application Protocol (CoAP)
Simple Object Access Protocol (SOAP)
Hypertext Transfer Protocol (HTTP)

Figure 5.2: IoT Network nodes - The communication protocols and IoT application protocols

In November 2021, CS Energy, already described in this document in ”3.2.1 Real examples of industry cyberattacks in 2021”, is an example of how critical infrastructure is becoming a target of ransomware attacks. The attack affected the ability of the Callide and Kogan Creek power plants to produce electricity. In response, CS Energy implemented business continuity plans and separated the corporate network from other internal networks. The plants cannot be stopped in this situation, which increases the probability of a negotiation to resume operations as soon as possible. Endpoint Detection and Response (EDR) is being used by companies to protect vital infrastructure against ransomware attacks, which have become a serious threat [63].

In March 2022, Bloomberg published an investigation into a massive hacking operation targeting the US energy sector, including liquefied natural gas. More than 100 computers owned by current and former employees of US energy companies such as Cheniere Energy, Chevron, EQT Corp. and Kinder Morgan, were compromised by hackers. While the investigation did not reveal whether the hackers managed to compromise the companies, Russia is likely to be the prime suspect. The motivation for the attack is likely state-sponsored and could compromise companies. Identifying hackers is challenging due to the importance of the targeted infrastructure and the timing of the attack [2].

In April 2022, liquefied natural gas facilities in Barcelona, Spain and Portugal were the most likely targets of a new malware known as Pipedream that the US government had recently discovered. The National Security Agency, the Department of Energy, the Infrastructure and Cybersecurity Agency and the FBI jointly issued a notice announcing the discovery of the system. While the FBI warned that it would take months or years to develop effective defences against the system, private security experts worked closely with government agencies to analyze it. The software is designed to exploit persistent vulnerabilities in defence control systems and industry requirements for compatibility between products manufactured by different vendors. Furthermore, it can be challenging to keep track of what is happening inside the physical equipment, and hundreds of different types of programmable logic controllers (PLCs) can be targeted. The attack kit is in keeping with Russia's historical interest and includes tools for sabotage, disruption and possibly physical destruction. As a result of the invasion, NATO and the EU pledged to decrease Russian oil and gas imports [110].

The cyber threat to the energy sector is rapidly growing and evolving, with frequent attacks, threats, and malware deployment. Given that businesses have no control over their supply chains and may have limited access to information or visibility regarding supply chain cyber risk, ICS is one of the most difficult vulnerabilities to address. Companies can begin addressing this by identifying and mapping critical assets, utilizing a cybersecurity maturity model, and developing a framework that is secure, watchful, and resilient. In order to share intelligence, take part in training exercises, create new standards and frameworks, and test out new technologies, they will be able to work together with peers, governments, suppliers, and other industrial sectors thanks to this. Electric energy businesses have a significant opportunity to lower risk for themselves, the energy industry, and society by utilizing these opportunities[101].

Chapter 6

Strengthen Essential Preventive Measures

6.1 Introduction

The security in organizations is not restricted to a local perimeter, the technological development results in a greater decentralization of resources and people, thus more exposure to internal and external threats [65]. It is essential to adopt and implement preventive measures to mitigate the risks of constant threats, such as all known forms of malware to which organizations are exposed. In section II, where ten attacks are listed, about six are identified as ransomware attacks, the remaining cases by acts of cyberattacks, security breaches, sabotage and exploitation of a vulnerability in the Apache Log4j software [163].

6.2 Hardware, Software and Ransomware

In 2021, a dozen security holes in the industrial WLAN hardware from German industrial solutions provider Weidmueller have been fixed. Vulnerabilities include the ability to escalate privileges, decrypt traffic, and run arbitrary code or take command. Because many of the weaknesses require authentication in order to be exploited, it is not immediately clear how the authentication bypass vulnerability is related to the other vulnerabilities. Weidmüller advises customers to install the most recent firmware if they want to protect their devices. The flaws, identified by the CVE numbers CVE-2021-33528 through

CVE-2021-33539, have the potential to be exploited to grant additional privileges, decrypt communications, run arbitrary code or commands, start denial-of-service attacks, and thwart authentication. It is unclear whether the authentication bypass vulnerability could be connected to other vulnerabilities given that many of the flaws require authentication to be exploited, at least with low privileges [92].

In November 2021, the Apache Software Foundation was alerted to a critical vulnerability in Apache Log4j [102], known as "Log4Shell", identified as vulnerability CVE-2021-44228 [36] and affects any version of Log4J before v2.15.0. It is a logging library used by many Java-based applications and implemented on millions of devices that allow code execution on vulnerable systems by unauthenticated remote users. To mitigate this critical vulnerability it´s vital to identify all assets that use the Log4j Java library offline or online and update them to the latest version. It is essential to monitor unusual traffic patterns to flag any malicious activity [15], such as outgoing JNDI LDAP/RMI traffic. Immediate actions to protect against Log4j exploitation [13]:

- Find all web-based resources that support data inputs, and use the Log4j Java library throughout the stack.
- Find out what resources employ the Log4j library.
- Adapted assets should be isolated or updated. Assume that you've been compromised, look for signs of malicious activity, and identify common post-exploit sources and activity.
- Keep an eye out for unusual traffic patterns, such as DMZ systems opening outbound connections or JNDI, LDAP, or RMI outbound traffic.

In 2022, ransomware attacks on industrial companies rose by 87%, with the manufacturing industry being the main target of the malicious software. One ransomware hacking tool could disable tens of thousands of systems that assist in the management of the world's electricity infrastructure, gas pipelines, and water companies. Hackers targeted the mining, food, water, electrical, and natural gas sectors. Organizations should develop strong response strategies, have tools for monitoring their infrastructure, and secure access to their systems by implementing two-factor authentication to protect themselves from attacks. In the last few weeks, ransomware attacks have hampered public school systems in Arizona and Massachusetts and interfered with derivatives training [146].

6.3 Vulnerabilities and associated risks to be aware

In chapter 3 of this document, the results of these attacks are briefly discussed and used as examples of the need for increased awareness of the vulnerabilities and associated risks that exist in the complex business context. It can have a negative impact on everyone's cybersecurity as well as the regular operation of any industry's services and those of its partners. As hackers become more skilled in their use of the same data tools and AI technology as those developing IoT systems, the risk of a data breach rises. There are specific areas within a factory and its connected systems where a breach, like unauthorized access, can happen. The risk of a data breach rises as hackers become more skilled at using the same data tools and AI technology as the manufacturers creating IoT systems. A breach, such as unauthorized access, can occur in particular locations within a factory and its connected systems. To ensure safety, it is important to review the following examples [96]:

- Insecure Web Interfaces: It has problems with weak default passwords, lockout and session management, and credential exposure within the network where users interact with IoT devices.

- Insecure Network Services: Attackers may be able to access the network directly from here thanks to open ports, buffer overflows, and Denial-of-Service attacks.

- Weak Encryption: When data is transferred between devices, weak encryption or, in some cases, no encryption, can give hackers the ability to collect data.

- Insecure Mobile Interfaces: Mobile interfaces experience the same encryption and authentication problems as desktop interfaces because so many businesses offer field service as an addition to their manufacturing operation for repair and maintenance.

6.4 Cybersecurity incident trends to be aware

1,063 security incidents were reported in 2022, accounting for 480,014,323 compromised records, a 14.8% decrease from 2021. But the number of reported incidents fell significantly in the first half of the year, before rising again from July to December. This illustrates the state of cyber security because hackers constantly come up with new ways to get around defences and switch to new schemes [74]. With cybersecurity incidents expected to result in damage, trends that organizations need to be aware of are [148]:

- Increased use of hardware - Software programs enable businesses to achieve great results and form new strategies, but they are attractive to cybercriminals. As a result, hardware is expected to gather speed, but businesses should not reduce investments in upgraded software.
- Remote work attacks - With hackers continuously developing strategies to exploit potential network vulnerabilities and downtime, cyberattacks targeting remote workers are anticipated to significantly increase.
- Growing government interest: Massive cyberattacks against high-priority targets have drawn the attention of international government agencies, spurred increased investment, and prompted new regulations.
- Ransomware targeting SMBs: The size of the business does not usually matter to cyber criminals. Ransomware organizations will turn their attention to small and medium-sized businesses (SMBs), which have less resources, staff, and security expertise, as governments increase investment to protect critical infrastructure.
- The rise of AI defenses: Organizations must strengthen their defenses as a result of the sophistication of various cybersecurity incidents rising. Smarter, quicker, and more proactive security will be made possible by AI-powered solutions, filling in the gaps in the cybersecurity sector.

6.5 Precautions against ransomware attacks

The FBI has informed Food and Agriculture (FA) industry partners that ransomware actors may be more likely to target agricultural cooperatives during critical planting and harvest seasons, disrupting operations, causing financial loss and negatively impacting the food supply chain. Cyber actors may perceive cooperatives as lucrative targets willing to pay due to their time-sensitive role in agricultural production. The frequency of ransomware attacks against the entire farm-to-table spectrum of the FA sector is remarkable. Observing the following precautions, these are applicable to any industry, so to mitigate the threat and improve the defense against ransomware attacks these are the precautions against ransomware attacks suggested [49]:

- Back up your data frequently and password-protect offline backup copies. Make sure copies of crucial data are inaccessible on the system where they are stored for modification or deletion.
- Implement a recovery plan that includes keeping several copies of proprietary or sensitive data and servers in a geographically distinct, segmented location (i.e., hard drive, storage device, the cloud).
- Develop an operations strategy for the event that systems fail by identifying critical functions. In case manual operation is required, consider your options.
- Segment your network and use it.
- As soon as updates and patches are available, apply them to firmware, software, and operating systems.
- Anytime you can, use multifactor authentication, use secure passwords, change them frequently, and set the shortest time between changes for network systems and accounts. A strong passphrase should be used whenever possible in place of reusing the same password across multiple accounts.
- Remote access/RDP ports that aren't in use should be disabled, and logs should be kept.

- Audit user accounts with elevated or administrative privileges, configure access controls with the least amount of privilege in mind, and Install software only with administrator access.
- Every host should have antivirus and anti-malware software installed and updated frequently.
- Use only private Wi-Fi networks; stay away from open ones. Use a virtual private network by setting one up (VPN).
- Emails sent from outside your organizations might benefit from an email banner and Block links in emails you've received.
- Emphasize education and awareness about cyber security. Train users on information security principles and practices as well as general, emerging cybersecurity risks and vulnerabilities, such as ransomware and phishing scams, on a regular basis.

6.6 Data breach success...security failure

Although cybersecurity defences have significantly improved, cyberattacks and data breaches remain a significant business. According to the Identity Theft Resource Center, the number of data breaches in the first quarter increased by 14% from a year earlier (ITRC). This rise is in line with the 68% increase in breaches from 2020 to 2021 [176]. Kaspersky advises taking the following actions to guarantee accurate staff usage of corporate data:

- If at all possible, limit who has access to vital corporate information, thereby limiting the amount of information that is accessible to all staff. Organizations with a high employee-to-confidential information-to-be-sold or otherwise-used ratio are more likely to experience breaches.
- Establish a policy for accessing corporate resources, such as email accounts, shared folders, and online documents. Maintain it, and block access if a worker leaves the company. Utilize cloud access security broker software to manage, track, and enforce security guidelines for employee activity within cloud services;

- To ensure that corporate information is safe in the event of an emergency, regularly backup important data;
- Clearly define the rules for using resources and services from outside sources. The appropriate tools to use and why should be made clear to staff. Any new software that is used for work should have a clear approval process with IT and other responsible roles;
- Encourage staff to regularly change their passwords and use strong passwords for all online accounts they have;
- Inform staff on a regular basis of the value of adhering to fundamental cybersecurity guidelines for secure email, web browsing, and account management;
- Employ dedicated cybersecurity services which provide visibility over cloud services used by staff.

Chapter 7

Conclusions

The last 20 years have emerged significant developments in industrial production and development, with new technologies, networks and emerging production systems due to the development of the internet and new distributed adaptive production systems. These architectures resulted in improved service activities, new business models and increased demand and offering of goods, resulting in fewer interactions among production system participants.

The industrial sector has become increasingly dependent on data for processes related to the production and management of all inherent resources. This technological update has generated increasing complexity, as described throughout Chapter 2, through the constant input and output of fundamental data for the planning, management and control of an industrial unit. Still, in chapter 2, a survey of a group of 30 professionals is documented in the collection of data on the convergence between IT/OT in their organizations. After analyzing the data received, in general, they reveal a positive awareness of the importance of integrating information technologies with operational technologies in the context of an industrial unit.

Cybersecurity is increasingly crucial to the industry 4.0 technology ecosystem due to the exponential use of IoT devices and embedded systems. Industry 4.0 should reinforce awareness of the need to review and update its cybersecurity policies in shorter cycles. It is critical to prepare for new threats and possible risks, prioritizing planning based on their impact. With special attention to interactions through data networks between different devices, people and products.

The frameworks presented, throughout chapter 4, aim to guide through security rules and procedures in improving the effectiveness and efficiency of strategies in defence against the threats described in the attacks referenced in “3.3 Cyber attacks on industry and their consequences”.

Industrial activity has specific risks, as well as different risk tolerances and vulnerabilities, which must be analyzed in the context of each industry. Therefore, a fundamental framework for recognizing, controlling, and presenting cybersecurity risks is needed. Thus, in Chapter 4, a set of frameworks and standards is suggested for identifying and naming specific vulnerabilities, as well as for classifying and describing the types of weaknesses that can lead to vulnerabilities. They are, in essence, a set of instruments to be taken into account during the development of a strategic approach to cybersecurity, as well as in the definition of its security policies so that they are effectively adapted to the context of each organisation.

Any industry needs energy, so renewable energy sources should be prioritized because energy production has an impact on the environment. Energy systems must therefore integrate distributed technology and sustainable energy. The sustainability and interoperability of smart grids, which use automation, communication, and IT/OT systems to control and monitor energy flows, are briefly discussed in chapter 5. These systems, which include interconnected sensors, network devices, and smart meters, among others, are critical infrastructures, but they are also becoming more frequent targets for groups of attackers who take advantage of the various layers of system architectures to intentionally cause harm or economic advantage.

In chapter 6, a set of essential preventive measures is presented to prevent ransomware attacks, to strengthen security on vulnerabilities and associated risks, how to avoid a data breach and what are the trends of cybersecurity incidents. All these threats can generate unpredictable negative impacts, as is the case, for example, with the ransomware attacks described in Chapter 3.

IT/OT convergence is expected to significantly improve the effectiveness of cybersecurity in preventing increasingly sophisticated attacks, as well as the escalating prevalence of ongoing cyber threats. Thus, this thesis intends to alert decision-makers in organizations to the growing dangers associated with outdated cybersecurity strategies.

This document recommends the need for organizations with an industrial component to review and update their cybersecurity strategies in shorter review cycles, in order to safeguard business continuity with enhanced and updated security.

As future work, research work on IT/OT convergence should be done in more depth to a broader group of technology professionals from different industries, on a set of questions that could be about the following topics:

- How do they review business continuity and disaster recovery plans?
- How do you assess the Vulnerabilities?
- How do you review governance, controls, roles and responsibilities?
- How do they quantify the financial loss associated with an incident, breach or disruption?
- Do you organize incident response drills?
- How do you review contractual protections and all insurance policies to ensure coverage for financial losses resulting from damage sustained in cyberattacks?
- What are the fully automated risk assessment and measurement platforms to identify, prioritize and focus risk mitigation efforts?
- To improve financial management, and timely decision-making, cybersecurity is becoming more complex. Does this start calling for automated solutions?

After collecting data through a survey with more technical questions, it would be interesting to analyze and build a broad view of the challenges that the industry is going through in this period of digital transformation and the integration of different information and operational technologies in a real business context.

References

[1] *2021 IoT Security Landscape - SAM Seamless Network*. en-US. Section: All. Apr. 2022. URL: `https://securingsam.com/2021-iot-security-landscape/` (visited on 10/29/2022).

[2] *21 U.S. LNG producers hacked*. en-GB. Section: Uncategorized. Apr. 2022. URL: `https://incyber.org/en/21-u-s-lng-producers-hacked/` (visited on 02/23/2023).

[3] *5 Most Common Types of Ransomware — CrowdStrike*. en. URL: `https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/` (visited on 02/18/2023).

[4] *A first step toward more agile hardware design, debugging*. en-US. URL: `https://cse.engin.umich.edu/stories/a-first-step-toward-more-agile-hardware-design-debugging/` (visited on 07/08/2022).

[5] Lillian Ablon. *Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data*. RAND, 2018.

[6] *AGCO ransomware attack disrupts tractor sales during U.S. planting season — Reuters*. URL: `https://www.reuters.com/business/agco-says-some-production-facilities-hit-by-ransomware-attack-2022-05-06/` (visited on 01/17/2023).

[7] Cristina Alcaraz. "Secure interconnection of IT-OT networks in industry 4.0". In: *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies* (2019), pp. 201–217.

[8] Rasim Alguliyev and Rasim Mahmudov. "Topical Issues of Regulation of Economic Relations in Internet Environment". In: *Economics* 4.1 (2016), pp. 25–36.

[9] Md Iman Ali and Sukhkirandeep Kaur. “Next-generation digital forensic readiness BYOD framework”. In: *Security and Communication Networks* 2021 (2021), pp. 1–19.

[10] Anton Allen, Ethan Puchaty, and Behbood Zoghi. “Challenges Cybersecurity Architects Are Facing In A Cloud Computing Environment”. In: *International Journal of Computer Science and Information Security (IJCSIS)* 19.6 (2021).

[11] David Wagner Soares de Almeida. “Levantamento da percepção de gestores sobre os desafios e benefícios na implantação de plataformas digitais na direção de uma cidade inteligente: o caso de maricá”. PhD thesis. Universidade Federal do Rio de Janeiro, 2022.

[12] Joseph Amankwah-Amoah et al. “COVID-19 and digitalization: The great acceleration”. In: *Journal of Business Research* 136 (2021), pp. 602–611.

[13] *Apache Log4j Vulnerability Guidance CISA*. URL: `https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance` (visited on 04/11/2022).

[14] Nuno Araújo, Vânia Pacheco, and Leonardo Costa. “Smart Additive Manufacturing: The Path to the Digital Value Chain”. In: *Technologies* 9.4 (2021), p. 88.

[15] Mohammed Asiri, Neetesh Saxena, and Peter Burnap. “Investigating usable indicators against cyber-attacks in industrial control systems”. In: *Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS)*. 2021, pp. 1–5.

[16] AA Athulya and K Praveen. “Towards the detection of phishing attacks”. In: *2020 4th international conference on trends in electronics and informatics (ICOEI)(48184)*. IEEE. 2020, pp. 337–343.

[17] Sinchul Back and Rob T Guerette. “Cyber place management and crime prevention: the effectiveness of cybersecurity awareness training against phishing attacks”. In: *Journal of contemporary criminal justice* 37.3 (2021), pp. 427–451.

[18] Deval Bhamare et al. “Cybersecurity for industrial control systems: A survey”. In: *computers & security* 89 (2020), p. 101677.

[19] Shawn Bilak and Kaitlin Brennan. *Cybersecurity Capability Maturity Model (C2M2)-Cybersecurity Maturity Model Certification (CMMC) Supplemental Guidance (Draft).* Tech. rep. CARNEGIE-MELLON UNIV PITTSBURGH PA, 2022.

[20] Mary Bispham et al. “Cybersecurity in working from home: An exploratory study”. In: *TPRC49: The 49th Research Conference on Communication, Information and Internet Policy.* 2021.

[21] Jenny Blessing, Jules Drean, and Sarah Radway. “Survey and analysis of US policies to address ransomware”. In: (2022).

[22] Debra J Borkovich and Robert Joseph Skovira. “CYBERSECURITY INERTIA AND SOCIAL ENGINEERING: WHO’S WORSE, EMPLOYEES OR HACKERS?” In: *Issues in Information Systems* 20.3 (2019).

[23] Gustavo Andrade Bruzzeguez, Clóvis Neumann, and João Carlos Félix Souza. “O hardware comprometido: uma importante ameaça a ser considerada pela atividade de inteligência”. In: *Revista Brasileira de Inteligência* 13 (2018), pp. 113–127.

[24] Javaid Butt. “A conceptual framework to support digital transformation in manufacturing using an integrated business process management approach”. In: *Designs* 4.3 (2020), p. 17.

[25] *Canadian mining firm shuts down mill after ransomware attack.* URL: `https://www.bleepingcomputer.com/news/security/canadian-mining-firm-shuts-down-mill-after-ransomware-attack/` (visited on 02/07/2023).

[26] Alvaro Cardenas. “Cyber-physical systems security knowledge area issue”. In: *The Cyber Security Body Of Knowledge.* 1.0 ().

[27] *Ch: Siegfried affected by attack on its IT systems.* en-US. URL: `https://www.databreaches.net/ch-siegfried-affected-by-attack-on-its-it-systems/` (visited on 11/27/2022).

[28] Baotong Chen et al. “Smart factory of industry 4.0: Key technologies, application case, and challenges”. In: *Ieee Access* 6 (2017), pp. 6505–6519.

[29] Yulia Cherdantseva et al. “A review of cyber security risk assessment methods for SCADA systems”. In: *Computers & security* 56 (2016), pp. 1–27.

[30] Kam-Fung Cheung, Michael GH Bell, and Jyotirmoyee Bhattacharjya. "Cybersecurity in logistics and supply chain management: An overview and future research directions". In: *Transportation Research Part E: Logistics and Transportation Review* 146 (2021), p. 102217.

[31] *Community Resources: What Is a Smart Grid and How Did It Change Our Communities?* en-US. Sept. 2021. URL: `https://www.elevatenp.org/communities/community-resources-what-is-a-smart-grid-and-how-did-it-change-our-communities/` (visited on 02/22/2023).

[32] Angelo Corallo, Mariangela Lazoi, and Marianna Lezzi. "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts". In: *Computers in industry* 114 (2020), p. 103165.

[33] Addie Cormier and Christopher Ng. "Integrating cybersecurity in hazard and risk analyses". In: *Journal of Loss Prevention in the Process Industries* 64 (2020), p. 104044.

[34] Giovanna Culot et al. "Addressing industry 4.0 cybersecurity challenges". In: *IEEE Engineering Management Review* 47.3 (2019), pp. 79–86.

[35] *CVE - Home.* URL: `https://cve.mitre.org/cve/` (visited on 06/02/2022).

[36] *CVE-2021-44228 - GitHub Advisory Database.* URL: `https://github.com/advisories/GHSA-jfh8-c2jp-5v3q` (visited on 04/01/2022).

[37] *CWE - CWE List Version 4.8.* URL: `https://cwe.mitre.org/data/index.html` (visited on 06/03/2022).

[38] "Cybersecurity for Smart Grid Systems". en. In: *NIST* (). Last Modified: 2021-05-04T09:18-04:00. URL: `https://www.nist.gov/programs-projects/cybersecurity-smart-grid-systems` (visited on 02/20/2023).

[39] Baudouin Dafflon, Nejib Moalla, and Yacine Ouzrout. "The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: a literature review". In: *The International Journal of Advanced Manufacturing Technology* 113 (2021), pp. 2395–2412.

[40] Kelley Dempsey, Gregory Witte, and Doug Rike. *Summary of NIST SP 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations.* Tech. rep. National Institute of Standards and Technology, 2014.

[41] Lubna Luxmi Dhirani, Eddie Armstrong, and Thomas Newe. “Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap”. In: *Sensors* 21.11 (2021), p. 3901.

[42] Jianguo Ding et al. “Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions”. In: *Energies* 15.18 (2022), p. 6799.

[43] Anca Dinicu, Romana Oancea, and Ghiță Bârsan. “The Multidimensional Impact on Society of Cyber Attacks Targeting the Energy Critical Infrastructure Sector”. In: *Land Forces Academy Review* 26.4 (2021), pp. 406–417.

[44] Michael Dodson. “Capability-based access control for cyber physical systems”. PhD thesis. University of Cambridge, 2021.

[45] James Douet. “The Heritage of the Oil Industry”. In: *TICCIH–The International Committee for the Conservation of the Industrial Heritage* (2019).

[46] Renee Dudley and Daniel Golden. “The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms”. In: *MIT Technology Review and ProPublica* (2021).

[47] Zakaria El Mrabet et al. “Cyber-security in smart grid: Survey and challenges”. In: *Computers & Electrical Engineering* 67 (2018), pp. 469–482.

[48] *Essentials for an Effective Cybersecurity Audit.* URL: `https://www.isaca.org/resources/news-and-trends/industry-news/2022/essentials-for-an-effective-cybersecurity-audit` (visited on 06/08/2022).

[49] *FBI Private Industry 2022-04-20 - Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons.* URL: `https://www.ic3.gov/Media/News/2022/220420-2.pdf` (visited on 02/16/2023).

[50] Prajeet Nair• February 8 and 2023. *Ransomware Attack Disrupts Operations at MKS Instruments.* en. URL: `https://www.bankinfosecurity.com/ransomware-`

attack-disrupts-operations-at-mks-instruments-a-21153 (visited on 02/21/2023).

[51] Pietro Ferrara et al. "Static analysis for discovering IoT vulnerabilities". In: *International Journal on Software Tools for Technology Transfer* 23 (2021), pp. 71–88.

[52] *Ferrari denies breach following 7GB of data posted online.* URL: https://www.cshub.com/attacks/news/ferrari-denies-breach-following-7gb-of-data-posted-online (visited on 01/14/2023).

[53] Barbara Filkins, Doug Wylie, and AJ Dely. "Sans 2019 state of ot/ics cybersecurity survey". In: *SANS™ Institute* (2019).

[54] Karsten Friis, Lilly Pijnenburg Muller, and Lars Gjesvik. "Cyber-weapons in International Politics: Possible sabotage against the Norwegian petroleum sector". In: *NUPI report* (2018).

[55] Erick Galinkin, John Carter, and Spiros Mancoridis. "Evaluating attacker risk behavior in an internet of things ecosystem". In: *Decision and Game Theory for Security: 12th International Conference, GameSec 2021, Virtual Event, October 25–27, 2021, Proceedings 12.* Springer. 2021, pp. 354–364.

[56] Dragoş Glăvan et al. "Sniffing attacks on computer networks". In: *Scientific Bulletin" Mircea cel Batran" Naval Academy* 23.1 (2020), 202A–207.

[57] *Global Cybersecurity Outlook 2022.* URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2022/ (visited on 05/01/2022).

[58] Deborah Golden and Mary Galligan. *Cyber: New Challenges in a COVID-19–Disrupted World.* English. Nov. 2020. URL: https://corpgov.law.harvard.edu/2020/11/23/cyber-new-challenges-in-a-covid-19-disrupted-world/ (visited on 12/30/2022).

[59] Avi Gopstein et al. "Benefits of Smart Grid Interoperability". In: (2022).

[60] Avi Gopstein et al. *NIST framework and roadmap for smart grid interoperability standards, release 4.0.* Department of Commerce. National Institute of Standards and Technology ..., 2021.

[61] Alison C Graab. "The smart grid: a smart solution to a complicated problem". In: *Wm. & Mary L. Rev.* 52 (2010), p. 2051.

[62] Zhixing Gu. "History review of nuclear reactor safety". In: *Annals of Nuclear Energy* 120 (2018), pp. 682–690.

[63] The Gurus. *Expert comment: CS Energy ransomware attack.* en-US. Dec. 2021. URL: `https://www.itsecurityguru.org/2021/12/03/expert-comment-cs-energy-ransomware-attack/` (visited on 02/23/2023).

[64] Janusz Hajda, Ryszard Jakuszewski, and Szymon Ogonowski. "Security Challenges in Industry 4.0 PLC Systems". In: *Applied Sciences* 11.21 (2021), p. 9785.

[65] Abir Al-Harrasi, Abdul Khalique Shaikh, and Ali Al-Badi. "Towards protecting organisations' data by preventing data theft by malicious insiders". In: *International Journal of Organizational Analysis* ahead-of-print (2021).

[66] Shayan Hashemi and Mika Mäntylä. "Detecting anomalies in software execution logs with siamese network". In: *arXiv preprint arXiv:2102.01452* (2021).

[67] Christa Hoffmann et al. "Cyberattacks in agribusiness". In: *42. GIL-Jahrestagung, Künstliche Intelligenz in der Agrar-und Ernährungswirtschaft* (2022).

[68] Andreas Hohenegger et al. "Security certification experience for industrial cyber-physical systems using Common Criteria and IEC 62443 certifications in certMILS". In: *2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*. IEEE. 2021, pp. 25–30.

[69] Roger N Holden. "The Origins of the Power Loom Revisited". In: *The International Journal for the History of Engineering & Technology* 84.2 (2014), pp. 135–159.

[70] Elvis Hozdić. "Smart factory for industry 4.0: A review". In: *International Journal of Modern Manufacturing Technologies* 7.1 (2015), pp. 28–35.

[71] *IBM Report: Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year.* en-us. URL: `https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year` (visited on 08/11/2022).

[72] *IBM Security Study Finds Employees New to Working from Home Pose Security Risk*. en-us. URL: https://newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-Employees-New-to-Working-from-Home-Pose-Security-Risk (visited on 07/01/2022).

[73] Prasanna Kumar Illa and Nikhil Padhi. “Practical guide to smart factory transition using IoT, big data and edge analytics”. In: *Ieee Access* 6 (2018), pp. 55162–55170.

[74] Luke Irwin. *Data Breaches and Cyber Attacks in 2022*. pt. Jan. 2023. URL: https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-in-2022-408-million-breached-records (visited on 02/23/2023).

[75] *ISA99, Industrial Automation&Control Sys Security- ISA*. en. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99 (visited on 09/02/2022).

[76] *ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary*. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (visited on 08/08/2022).

[77] *ISO/IEC 27036-1:2021(en), Cybersecurity — Supplier relationships — Part 1: Overview and concepts*. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27036:-1:ed-2:v1:en (visited on 08/11/2022).

[78] Ahmad Issa et al. “Industrie 4.0 roadmap: Framework for digital transformation based on the concepts of capability maturity and alignment”. In: *Procedia Cirp* 72 (2018), pp. 973–978.

[79] Zahra Jadidi and Yi Lu. “A threat hunting framework for industrial control systems”. In: *IEEE Access* 9 (2021), pp. 164118–164130.

[80] B Jakobsen et al. “‘Challenges to effective EU cybersecurity policy—Briefing paper”. In: *Eur. Court Audit* (2019), pp. 1–74.

[81] Luke Kane et al. “Network Architecture and Authentication Scheme for LoRa 2.4 GHz Smart Homes”. In: *IEEE Access* 10 (2022), pp. 93212–93230.

[82] Amey Kanunje et al. “Penetration Testing and Vulnerability Assessment”. In: ().

[83] Ilker Kara and Murat Aydos. “The rise of ransomware: Forensic analysis for windows based ransomware attacks”. In: *Expert Systems with Applications* 190 (2022), p. 116198.

[84] Jasmeet Kaur. “Taxonomy of malware: virus, worms and trojan”. In: *Int. J. Res. Anal. Rev* 6.1 (2019), pp. 192–196.

[85] Mazaher Kianpour. “Socio-Technical Root Cause Analysis of Cyber-enabled Theft of the US Intellectual Property–The Case of APT41”. In: *arXiv preprint arXiv:2103.04901* (2021).

[86] Hokeun Kim and Edward A Lee. “Authentication and Authorization for the Internet of Things”. In: *IT Professional* 19.5 (2017), pp. 27–33.

[87] Jin Ho Kim. “A review of cyber-physical system research relevant to the emerging IT trends: industry 4.0, IoT, big data, and cloud computing”. In: *Journal of industrial integration and management* 2.03 (2017), p. 1750011.

[88] Moshe C Kinn. “Paramount importance of using distributed extra-low direct current voltage in the built environment”. In: *The Journal of Engineering* 2019.16 (2019), pp. 788–793.

[89] Alexander Kolpakov et al. “Transportation Fuel Resiliency: Case Study of Tampa Bay”. In: *Transportation Research Record* 2676.1 (2022), pp. 655–665.

[90] John Koon. *Solving Problems With The IoT*. en-US. Feb. 2023. URL: `https://semiengineering.com/solving-problems-with-the-iot/` (visited on 02/22/2023).

[91] Kazimierz T Kosmowski. “Business continuity management framework for Industry 4.0 companies regarding dependability and security of ICT and ICS/SCADA system”. In: *Safety and Reliability of Systems and Processes* (2021).

[92] Eduard Kovacs. *Weidmueller Patches Dozen Vulnerabilities in Industrial WLAN Devices*. en-US. June 2021. URL: `https://www.securityweek.com/weidmueller-patches-dozen-vulnerabilities-industrial-wlan-devices/` (visited on 02/16/2023).

[93] Nozomi Networks Labs. *Enhancing Threat Intelligence with the MITRE ATT&CK Framework*. en-US. Oct. 2021. URL: https://www.nozominetworks.com/blog/enhancing-threat-intelligence-with-the-mitre-attck-framework/ (visited on 02/19/2023).

[94] Mohammed Lalou, Mohammed Amin Tahraoui, and Hamamache Kheddouci. "The critical node detection problem in networks: A survey". In: *Computer Science Review* 28 (2018), pp. 92–117.

[95] Heiner Lasi et al. "Industry 4.0". In: *Business & information systems engineering* 6 (2014), pp. 239–242.

[96] Jacob Lauzier. *Industrial IoT Security: Challenges and Solutions*. en-us. URL: https://www.machinemetrics.com/blog/industrial-iot-security (visited on 02/20/2023).

[97] JooChan Lee, JangHoon Kim, and JungTaek Seo. "Cyber attack scenarios on smart city and their ripple effects". In: *2019 international conference on platform technology and service (PlatCon)*. IEEE. 2019, pp. 1–5.

[98] *LG U+ hit by second DDoS attack in a week*. URL: https://koreajoongangdaily.joins.com/2023/02/06/business/industry/Korea-LG-U-DDoS/20230206175514381.html (visited on 02/21/2023).

[99] Dan Li, Åsa Fast-Berglund, and Dan Paulin. "Current and future Industry 4.0 capabilities for information and knowledge sharing: Case of two Swedish SMEs". In: *The International Journal of Advanced Manufacturing Technology* 105 (2019), pp. 3951–3963.

[100] Joonas Linnosmaa et al. "Survey of cybersecurity standards for nuclear instrumentation and control systems". In: *International Symposium on Future I&C for Nuclear Power Plants, ISOFIC 2021: Online*. Okayama University. 2021.

[101] Steve Livingston et al. "Managing cyber risk in the electric power sector". In: *Deloitte. As of* 17 (2019).

[102] *Log4j – Apache Log4j Security Vulnerabilities*. URL: https://logging.apache.org/log4j/2.x/security.html (visited on 03/11/2022).

[103] *Los Mossos investigan un ciberataque al grupo Llobet.* es. URL: `https://cronicaglobal.elespanol.com/creacion/vida-tecky/mossos-investigan-ciberataque-grupo-llobet-bloquea-contabilidad_595756_102.html` (visited on 01/27/2023).

[104] Yang Lu. "Blockchain: A survey on functions, applications and open issues". In: *Journal of Industrial Integration and Management* 3.04 (2018), p. 1850015.

[105] Somayya Madakam et al. "Internet of Things (IoT): A literature review". In: *Journal of Computer and Communications* 3.05 (2015), p. 164.

[106] *Man in the Middle (MITM) Attacks — Types, Techniques, and Prevention.* en. URL: `https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/` (visited on 02/19/2023).

[107] Steve Mansfield-Devine. "Nation-state hacking–a threat to everyone". In: *Computer Fraud & Security* 2018.8 (2018), pp. 17–20.

[108] Soujanya Mantravadi et al. "Securing IT/OT links for low power IIoT devices: design considerations for industry 4.0". In: *IEEE Access* 8 (2020), pp. 200305–200321.

[109] *Medium-sized company Fritzmeier Group hit by cyber attack - B2B Cyber Security.* URL: `https://b2b-cyber-security.de/en/Mittelstaendler-Fritzmeier-Group-hit-by-cyber-attack/` (visited on 02/05/2023).

[110] Joseph Menn. "U.S. warns newly discovered malware could sabotage energy plants". en-US. In: *Washington Post* (Apr. 2022). ISSN: 0190-8286. URL: `https://www.washingtonpost.com/technology/2022/04/13/pipedream-malware-russia-lng/` (visited on 02/23/2023).

[111] Karl-Erik Michelsen. "Industry 4.0 in Retrospect and in Context". In: *Technical, Economic and Societal Effects of Manufacturing 4.0: Automation, Adaption and Manufacturing in Finland and Beyond* (2020), pp. 1–14.

[112] David Philip Miller and Debbie Rudder. "A 'revolver'evolving: the careers of a Boulton & Watt rotative steam engine at the Whitbread Brewery, London and the Powerhouse Museum, Sydney, 1784–2020". In: *The International Journal for the History of Engineering & Technology* 89.1-2 (2020), pp. 238–263.

[113] Michael JA Miranda. "Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach". In: *International Management Review* 14.2 (2018), pp. 5–10.

[114] Jozef Mocnej et al. "Decentralised IoT architecture for efficient resources utilisation". In: *IFAC-PapersOnLine* 51.6 (2018), pp. 168–173.

[115] Mamad Mohamed. "Challenges and benefits of industry 4.0: An overview". In: *International Journal of Supply and Operations Management* 5.3 (2018), pp. 256–265.

[116] Abubakar Sadiq Mohammed et al. "Cybersecurity challenges in the offshore oil and gas industry: an Industrial Cyber-Physical Systems (ICPS) perspective". In: *ACM Transactions on Cyber-Physical Systems (TCPS)* 6.3 (2022), pp. 1–27.

[117] Jeff Morgan et al. "Industry 4.0 smart reconfigurable manufacturing machines". In: *Journal of Manufacturing Systems* 59 (2021), pp. 481–506.

[118] *Morgan Advanced Materials cyberattack is "data security incident"*. URL: `https://techmonitor.ai/technology/cybersecurity/morgan-advanced-materials-cyberattack` (visited on 02/07/2023).

[119] *Most frequently reported types of cyber crime 2021- Statista*. en. URL: `https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime/` (visited on 07/27/2022).

[120] Valentin Mullet, Patrick Sondi, and Eric Ramat. "A review of cybersecurity guidelines for manufacturing factories in industry 4.0". In: *IEEE Access* 9 (2021), pp. 23235–23263.

[121] Glenn Murray, Michael N Johnstone, and Craig Valli. "The convergence of IT and OT in critical infrastructure". In: (2017).

[122] Aziz Naanani et al. "Security in Industry 4.0: Cyber-attacks and countermeasures". In: *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.10 (2021), pp. 6504–6512.

[123] "NIST Cybersecurity Framework". en. In: *NIST* (Nov. 2013). Last Modified: 2022-09-21T08:23-04:00. URL: https://www.nist.gov/cyberframework (visited on 07/30/2022).

[124] *Nvidia, the ransomware breach with some plot twists.* URL: https://www.malwarebytes.com/blog/news/2022/03/nvidia-the-ransomware-breach-with-some-plot-twists (visited on 01/05/2023).

[125] Mimi Enakome Oka and Martin Hromada. "Analysis of Current Preventive Approaches in the Context of Cybersecurity". In: *2022 IEEE International Carnahan Conference on Security Technology (ICCST)*. IEEE. 2022, pp. 1–5.

[126] Juliana Zúñiga Osorio and Álvaro Pachón De La Cruz. "Holistic vision of tools for transformation towards Industry 4.0". In: *2021 IEEE Colombian Conference on Communications and Computing (COLCOM)*. IEEE. 2021, pp. 1–6.

[127] Obinna G Otti. "Bring Your Own Device (BYOD): Risks to Adopters and Users". In: (2018).

[128] *Over 2.7 million cases of Emotet malware detected globally.* URL: https://english.kyodonews.net/news/2022/02/1b60294a9bb3-over-27-million-cases-of-emotet-malware-detected-globally.html (visited on 01/27/2023).

[129] *OWASP Foundation, the Open Source Foundation for Application Security — OWASP Foundation.* en. URL: https://owasp.org/ (visited on 10/12/2022).

[130] *OWASP Top 10:2021.* URL: https://owasp.org/Top10/ (visited on 10/21/2021).

[131] Harun Oz et al. "A survey on ransomware: Evolution, taxonomy, and defense solutions". In: *ACM Computing Surveys (CSUR)* 54.11s (2022), pp. 1–37.

[132] Serkan Ozkan. "CVE security vulnerability database". In: *Security vulnerabilities, exploits, references and more* ().

[133] Ercan Oztemel and Samet Gursev. "Literature review of Industry 4.0 and related technologies". In: *Journal of intelligent manufacturing* 31 (2020), pp. 127–182.

[134] T Pereira, L Barreto, and A Amaral. "Network and information security challenges within Industry 4.0 paradigm". In: *Procedia manufacturing* 13 (2017), pp. 1253–1260.

[135] Rodney Petersen et al. "Workforce framework for cybersecurity (NICE framework)". In: (2020).

[136] *Pharmaceutical Company Novartis Has Been Hacked - IDStrong*. URL: `https://www.idstrong.com/sentinel/novartis-data-breach/` (visited on 01/27/2023).

[137] Heloise Pieterse. "The cyber threat landscape in South Africa: A 10-year review". In: *The African Journal of Information and Communication* 28 (2021), pp. 1–21.

[138] Michael Powell et al. *Protecting information and system integrity in industrial control system environments: cybersecurity for the manufacturing sector*. Tech. rep. National Institute of Standards and Technology, 2021.

[139] Iosif Progoulakis et al. "Perspectives on cyber security for offshore oil and gas assets". In: *Journal of Marine Science and Engineering* 9.2 (2021), p. 112.

[140] Goran D Putnik et al. "What is a Cyber-Physical System: Definitions and models spectrum". In: *Fme Transactions* 47.4 (2019), pp. 663–674.

[141] Noor Ahmed Qarabsh, S Sabah Sabry, and H Ahmed Qarabash. "Smart grid in the context of industry 4.0: An overview of communications technologies and challenges". In: *Indonesian Journal of Electrical Engineering and Computer Science* 18.2 (2020), pp. 656–665.

[142] *Qulliq Energy Corporation impacted by a cybersecurity incident — Qulliq Energy Corporation*. URL: `https://www.qec.nu.ca/qulliq-energy-corporation-impacted-cybersecurity-incident` (visited on 02/02/2023).

[143] Petar Radanliev et al. "Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0". In: *Living in the Internet of Things: Cybersecurity of the IoT-2018*. IET. 2018, pp. 1–6.

[144] *Ransomware attack against Yum! Brands follows several incidents targeting restaurant industry*. en-US. URL: `https://www.cybersecuritydive.com/news/ransomware-yum-brands-restaurant-cyber/640843/` (visited on 02/23/2023).

[145] *Ransomware attack on data firm ION could take days to fix -sources — Reuters.* URL: `https://www.reuters.com/technology/ransomware-attack-data-firm-ion-could-take-days-fix-sources-2023-02-02/` (visited on 02/20/2023).

[146] *Ransomware attacks on industrial firms jumped 87 per cent in 2022.* en. Section: Tech. Feb. 2023. URL: `https://www.scmp.com/tech/tech-trends/article/3210241/ransomware-attacks-industrial-firms-jumped-87-cent-2022-hitting-renewable-energy-and-utilities` (visited on 02/23/2023).

[147] Awais Rashid et al. "The Cyber Security Body of Knowledge". en. In: ().

[148] *Recent Cyber Attacks in 2022.* en. URL: `https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks` (visited on 02/23/2023).

[149] Anna Ribeiro. *Ransomware activity in industrial environments almost doubles, with over 70% focused on manufacturing sector.* en-US. Feb. 2023. URL: `https://industrialcyber.co/ransomware/ransomware-activity-in-industrial-environments-almost-doubles-with-over-70-focused-on-manufacturing-sector/` (visited on 02/20/2023).

[150] *Riviera - News Content Hub - DNV confirms ShipManager cyber attack hit 1,000 vessels.* URL: `https://www.rivieramm.com/news-content-hub/news-content-hub/dnv-reports-cyber-attack-on-its-shipmanager-software-74466` (visited on 02/16/2023).

[151] Scott Rose. *Planning for a Zero Trust Architecture: A Planning Guide for Federal Adminstrators.* Tech. rep. National Institute of Standards and Technology, 2022.

[152] Scott Rose et al. *Zero trust architecture.* Tech. rep. National Institute of Standards and Technology, 2020.

[153] Shahrin Sadik et al. "Toward a sustainable cybersecurity ecosystem". In: *Computers* 9.3 (2020), p. 74.

[154] Thilo Sauter. "The continuing evolution of integration in manufacturing automation". In: *IEEE Industrial Electronics Magazine* 1.1 (2007), pp. 10–19.

[155] IBM Security. "Cost of a data breach report 2021". In: *Risk Quantification* 73 (2021).

[156] *Service Organisation Controls – SOC 2 — Risk Advisory — Deloitte Southern Africa.* en. URL: `https://www2.deloitte.com/za/en/pages/risk/articles/service-organisation-controls.html` (visited on 09/05/2022).

[157] Velizar Shalamanov. "Organizing for IT effectiveness, efficiency and cyber resilience in the academic sector: National and regional dimensions". In: *Information & Security: An International Journal* 42.1 (2019).

[158] Tohid Shekari. "Methods to attack and secure the power grids and energy markets". PhD thesis. Georgia Institute of Technology, 2021.

[159] Akaki Shekeladze et al. "GEORGIAN EXPERIENCE OF DEVELOPING CYBER CAPABILITIES IN THE DEFENCE FIELD". In: *Journal of Defense Resources Management (JoDRM)* 13.2 (2022), pp. 25–34.

[160] Anmol Singh and Bhaskar Kapoor. "Analysis of the human factor behind cyber attacks". In: *Int. Res. J. Eng. Technol.* 3.14 (2016), pp. 1166–1172.

[161] *Smart Grids – Analysis.* en-GB. URL: `https://www.iea.org/reports/smart-grids` (visited on 02/22/2023).

[162] *Snap-on Tools Hit by Cyberattack Claimed by Conti Ransomware Gang - SecurityWeek.* URL: `https://www.securityweek.com/high-end-tools-manufacturer-snap-discloses-data-breach/` (visited on 01/10/2023).

[163] Shreyas Srinivasa, Jens Myrup Pedersen, and Emmanouil Vasilomanolakis. "Deceptive directories and "vulnerable" logs: a honeypot study of the LDAP and log4j attack landscape". In: *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE. 2022, pp. 442–447.

[164] German Sternharz et al. "Self-Protected Virtual Sensor Network for Microcontroller Fault Detection". In: *Sensors* 22.2 (2022), p. 454.

[165] Kevin Stine, Matthew Barrett, et al. "Portuguese translation of the framework for improving critical infrastructure cybersecurity version 1.1 (cybersecurity framework)". In: *National Institute of Standards and Technology* (2021).

[166] Keith Stouffer et al. "Cybersecurity framework version 1.1 manufacturing profile". In: *National Institute of Standards and Technology: Gaithersburg, MD, USA* (2020).

[167] Keith Stouffer et al. *Guide to Operational Technology (OT) Security.* Tech. rep. National Institute of Standards and Technology, 2022.

[168] Blake E Strom et al. “Mitre att&ck: Design and philosophy”. In: *Technical report.* The MITRE Corporation, 2018.

[169] Ahmet Ali Süzen. “A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem.” In: *International Journal of Computer Network & Information Security* 12.1 (2020).

[170] *Techniques - ICS — MITRE ATT&CK®.* URL: `https://attack.mitre.org/techniques/ics/` (visited on 09/09/2022).

[171] Chee-Wooi Ten, Govindarasu Manimaran, and Chen-Ching Liu. “Cybersecurity for critical infrastructures: Attack and defense modeling”. In: *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 40.4 (2010), pp. 853–865.

[172] *The Cyber Defense Index 2022/23.* en. URL: `https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/` (visited on 11/16/2022).

[173] *The Human Factor Report 2022 - Threat Report — Proofpoint US.* en-us. Aug. 2021. URL: `https://www.proofpoint.com/us/resources/threat-reports/human-factor` (visited on 08/27/2022).

[174] *The State of OT/ICS Cybersecurity in 2022 and Beyond.* URL: `https://www.sans.org/white-papers/state-ics-ot-cybersecurity-2022-beyond/` (visited on 02/27/2023).

[175] Tetsuo Tomiyama. “Intelligent computer-aided design systems: Past 20 years and future 20 years”. In: *Ai Edam* 21.1 (2007), pp. 27–29.

[176] *Top 10 Data Breaches So Far in 2022 - Cybersecurity — Digital Forensics — Crypto Investigations.* en-US. Aug. 2022. URL: `https://ermprotect.com/blog/top-10-data-breaches-so-far-in-2022/,%20https://ermprotect.com/blog/top-10-data-breaches-so-far-in-2022/` (visited on 02/23/2023).

[177] Akihiro Tsuchiya et al. "Software defined networking firewall for industry 4.0 manufacturing systems". In: *Journal of Industrial Engineering and Management (JIEM)* 11.2 (2018), pp. 318–333.

[178] Tsvetan Tsvetanov and Srishti Slaria. "The effect of the Colonial Pipeline shutdown on gasoline prices". In: *Economics Letters* 209 (2021), p. 110122.

[179] *UK Metal Engineering Firm Vesuvius Hit by Cyber-Attack - Infosecurity Magazine.* URL: `https://www.infosecurity-magazine.com/news/uk-metalg-firm-vesuvius-cyberattack/` (visited on 02/20/2023).

[180] *Understanding CIA in an OT environment.* en. URL: `https://www.ace-net.com/blog/confidentiality-integrity-availability` (visited on 02/19/2023).

[181] Saurabh Vaidya, Prashant Ambad, and Santosh Bhosle. "Industry 4.0–a glimpse". In: *Procedia manufacturing* 20 (2018), pp. 233–238.

[182] Tharaka de Vass, Himanshu Shee, and Shah Jahan Miah. "IoT in supply chain management: Opportunities and challenges for businesses in early industry 4.0 context". In: *Operations and Supply Chain Management: An International Journal* 14.2 (2021), pp. 148–161.

[183] Wei Wang, Francesco Di Maio, and Enrico Zio. "Adversarial risk analysis to allocate optimal defense resources for protecting cyber–physical systems from cyber attacks". In: *Risk Analysis* 39.12 (2019), pp. 2766–2785.

[184] Zuoguang Wang, Hongsong Zhu, and Limin Sun. "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods". In: *IEEE Access* 9 (2021), pp. 11895–11910.

[185] Daniel Watson. "Fordism: A review essay". In: *Labor History* 60.2 (2019), pp. 144–159.

[186] Amy Deen Westbrook. "A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets and Defending National Security". In: *NYUJL & Bus.* 18 (2021), p. 391.

[187] *What is an Advanced Persistent Threat (APT)? — CrowdStrike*. en. URL: `https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/` (visited on 02/18/2023).

[188] *What is Industry 4.0 and how does it work? — IBM*. pt. URL: `https://www.ibm.com/topics/industry-4-0` (visited on 02/06/2023).

[189] H James Wilson, Sharad Sachdev, and Allan Alter. "How companies are using machine learning to get faster and more efficient". In: *Harvard Business Review* (2016).

[190] *X-Force Threat Intelligence Index 2022*. Tech. rep. IBM Security, Feb. 2022. URL: `https://www.ibm.com/downloads/cas/ADLMYLAZ`.

[191] Shanshan Yang et al. "Opportunities for industry 4.0 to support remanufacturing". In: *Applied Sciences* 8.7 (2018), p. 1177.

[192] Xingjie Yu and Huaqun Guo. "A survey on IIoT security". In: *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*. IEEE. 2019, pp. 1–5.

[193] Bing Zhang et al. "Efficiency and effectiveness of web application vulnerability detection approaches: A review". In: *ACM Computing Surveys (CSUR)* 54.9 (2021), pp. 1–35.

[194] Caiming Zhang and Yong Chen. "A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics". In: *Journal of Industrial Integration and Management* 5.01 (2020), pp. 165–180.

[195] Ray Y Zhong et al. "Intelligent manufacturing in the context of industry 4.0: a review". In: *Engineering* 3.5 (2017), pp. 616–630.

[196] Aaron Zimba et al. "Crypto mining attacks in information systems: An emerging threat to cyber security". In: *Journal of Computer Information Systems* (2018).

[197] Tiago Zonta et al. "Predictive maintenance in the Industry 4.0: A systematic literature review". In: *Computers & Industrial Engineering* 150 (2020), p. 106889.