energies

MDPI

*Review*

# Cybersecurity in Cyber–Physical Power Systems

**Luiz Fernando Ribas Monteiro [1,2], Yuri R. Rodrigues [3] and A. C. Zambroni de Souza [1,*]**

[1] Institute of Electrical System and Energy, Federal University of Itajuba, Itajuba 37500-903, MG, Brazil
[2] Engineering Department, Dom Bosco Educational Association, Resende 27523-000, RJ, Brazil
[3] Department of Engineering and Computer Science, Seattle Pacific University, Seattle, WA 98119, USA
* Correspondence: zambroni@unifei.edu.br

**Abstract:** The current energy transition combined with the modernization of power systems has provided meaningful transformations in the transmission, distribution, operation, planning, monitoring, and control of power systems. These advancements are heavily dependent on the employment of new computing and communications technologies, which, combined with traditional physical systems, lead to the emergence of cyber–physical systems (CPSs). In this sense, besides the traditional challenges of keeping a reliable, affordable, and safe power grid, one must now deal with the new vulnerabilities to cyberattacks that emerge with the advancement of CPSs. Aware of this perspective and the severity of the ongoing challenges faced by the industry due to cyberattacks, this paper aims to provide a comprehensive survey of the literature on cybersecurity in cyber–physical power systems. For this, clear definitions, historical timelines, and classifications of the main types of cyberattacks, including the concepts, architectures, and basic components that make up, as well as the vulnerabilities in managing, controlling, and protecting, a CPS are presented. Furthermore, this paper presents defense strategies and future trends for cybersecurity. To conduct this study, a careful search was made in relevant academic and industrial databases, leading to a detailed reporting of key works focused on mitigating cyberattacks and ensuring the cybersecurity of modern CPSs. Finally, the paper presents some standards and regulations that technical and international institutions on cybersecurity in smart grids have created.

**Keywords:** cybersecurity; cyber–physical systems; cyberattack; monitoring; control; protection; defense strategies; future trends; power systems; energy transition

check for updates

**Citation:** Ribas Monteiro, L.F.; Rodrigues, Y.R.; Zambroni de Souza, A.C. Cybersecurity in Cyber–Physical Power Systems. *Energies* **2023**, *16*, 4556. https://doi.org/10.3390/en16124556

Academic Editors: Javier Contreras and Surender Reddy Salkuti

Received: 7 April 2023
Revised: 12 May 2023
Accepted: 2 June 2023
Published: 7 June 2023

**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

The Industrial Revolution, which took place in the middle of the 18th century, changed the daily life of the population and made possible the production of large amounts of energy, products, and goods through the invention of the steam engine and the use of fossil fuels, which were the great driving force of this era. This historical period transitioned from small-scale handmade manufacturing to mass manufacturing with machines [1–3]. Due to society's changing habits and the parallel overuse of these fuels that were rich in coal, hydrocarbons, and later petroleum derivatives, the planet's temperature has gradually changed, as presented in countless measurements and studies carried out over time [4–7]. The global average temperature is a simple parameter used to measure the climatic changes that the planet goes through over time. Global warming is a phenomenon that directly influences this parameter. As the burning of fossil fuels develops, it promotes the increase of $CO_2$ concentration in the atmosphere and therefore increases the greenhouse effect and global warming [7,8]. The unregulated growth in the global average temperature entails numerous impacts on the planet. Reference [9] addresses a review of the literature about the impacts that climate change generates due to the increase in the planet's average temperature. In addition, this study addresses the effects that climate change brings to planet Earth, human life, and the environment. The increasing occurrence of emergency

events has also demanded new response action plans. Therefore, planning actions that can adapt to these climate changes must also be developed [10].

In [11], a perspective of climate change impacts from poorer countries' outlook is presented. This topic is extended in [12], pointing out that, in climate change, developed countries have become even richer, while poorer countries are economically penalized and suffer more from the environmental impacts. Therefore, the adverse effects are disproportionate and have increased economic disparities worldwide. Unregulated climate change harms all living beings on Earth due to the negative impacts imposed on the planet's sustainability [13]. In addition, the effects on the energy performance of city buildings are mostly influenced by how they are built and distributed in urban areas [14]. Thus, from an energy point of view, current climate change influences the planning and building design of future smart cities [15] and the technologies involved in those projects [16].

In this perspective, the diversification of power generation sources (use of renewable energy, e.g., solar and wind power), the insertion of electric vehicles (EVs), the use of new technologies, and the increasing reliability and robustness of the electric grid are current points of interest. These factors and the growing environmental concern have driven the progressive transformation of the traditional electric system in smart grids (SGs) [17–19]. This new and complex electric grid concept includes traditional and renewable energy sources, including intermittent generations, demand management characteristics, and a greater degree of management and distributed control requirement due to the bidirectional power flow possibility. This change from the conventional system to SGs has gradually occurred with the inclusion of structures known in the literature as microgrids (MGs). However, the widespread adoption of these changes in a global energy matrix scale still depends on the definition of multiple financial, technological, and regulatory aspects [17–19].

In addition, the advancement of 5G cellular network technology, the development of the Internet of Things, and the use of big data [20,21] have powered the development of the so-called Industry 4.0 [22] and advanced automated technologies systems [23–25] such as automatically guided vehicles, advanced industrial processes control systems, sustainable development solutions, and other technologies that use big sets of information to enhance in a transformative way our social organization. In this sense, our modern society is undergoing transformations that imply a greater interconnection between people and technology. Given this scenario, this interrelationship requires greater data acquisition, distribution, and storage security. Developed countries such as the United States (US) and the United Kingdom (UK) are proposing strategies to ensure the cybersecurity of these systems [26,27] to mitigate the number of cyber threats and achieve cyber resilience. Cyber resilience consists of the ability of a system to suffer cyberattacks and maintain the integrity, security, confidentiality, and availability of its data and services. In this new age of big data and advanced communication systems, cybersecurity is a complex challenge for the safe use and development of new technologies.

Seeking to meet the need for the integration of new sources of energy, the entry and integration of new technologies into the grid, global concerns about the environment, diversification of the energy matrix, and the growing consumption of energy, the electrical system is in the process of modernizing its operation, planning, maintenance, communication, management, and control. Therefore, the power system is gradually transforming into SGs, and consequently, the vulnerabilities of this new system become the target of cyberattacks. Thus, their cybersecurity becomes a critical issue in ensuring reliability and safety in the operation of power systems. Observing this problem, this paper presents a study on cybersecurity in the power cyber–physical system with a history and classification of the main cyberattacks available in the literature that target the electrical and industrial sectors in general. Due to the modernization and transformation of the power system, this paper also presents concepts, characteristics, and the vulnerabilities of the cyber–physical system. In this perspective, this paper aims to review the literature on the cybersecurity of electrical power systems and offer a clear perspective on key developments currently available in the academic and industrial literature. The paper also aims to contribute a

state-of-the-art study of cybersecurity applications in monitoring systems, control systems, and protection systems. For this study, a comprehensive search was performed in multiple academic and industrial database resources, including but not limited to Science Direct, IEEE Xplore, Google Scholar, MDPI databases, and others. In addition, this paper presents some of the major cybersecurity standards and regulations created by companies and technical and scientific organizations that aim to standardize, regulate, and enhance the security and reliability of smart grid operation.

Given this, this paper discusses many proposals, research strategies, techniques, and methodologies for preventing, detecting, investigating, correcting, and mitigating cyberattacks on industrial monitoring and control systems and fault relays in the power system. Thus, this paper seeks to fill this gap in the literature on cyber–physical power systems and to create a tool that assists in the prevention and correction of these types of attacks. With these cybersecurity goals in the operation of CPPS, this paper presents the following contributions.

- A robust review of the literature that is capable of guiding decision-making on a possible operational scenario in which the cyber–physical power system suffers cyber-attacks, indicating a possible solution to this problem.
- A theoretical framework capable of assisting in the planning and developing of cyber-security systems for cyber–physical systems.
- A tool to prevent and mitigate these types of attacks.
- A review of the layers, basic components, and key vulnerabilities of the devices that comprise the control and management system for cyber–physical systems.
- A robust history and the main types of cyberattacks against industrial systems, as well as the main standards and regulations developed for cybersecurity in microgrids.

The structure of the paper is organized as follows. Section 2 presents key concepts, historical timelines, and definitions of different types of cyberattacks. Section 3 discusses preliminary concepts and the basic layers, components, and the vulnerabilities in managing and controlling a CPS. Section 4 presents applications of cybersecurity in the monitoring and control system and in protection systems in power systems. Furthermore, it presents defense strategies and future trends for cybersecurity. Finally, Section 5 presents some standards and protocols created by scientific institutions on cybersecurity in smart grids. Section 6 makes the final considerations, giving this work's general contributions and suggestions for future works. Figure 1 provides the framework of the paper.

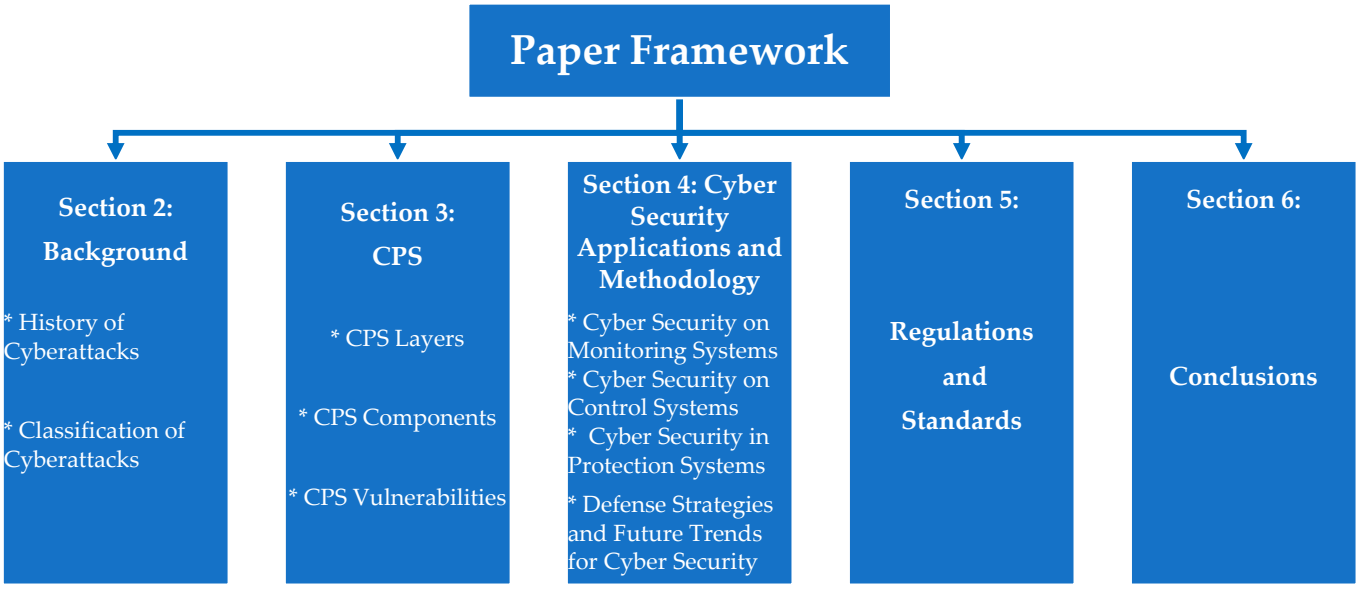


**Figure 1.** Paper framework.

## 2. Background

Cyberattacks are virtual actions that aim to infiltrate individuals' or organizations' computer networks, typically seeking to cause harm or disrupt service. These attacks can have different focuses, from compromising data integrity to stealing confidential information [28]. Therefore, developing adequate protection layers for a CPS is necessary to ensure the security and reliable operation of power and energy systems. Still, during recent years, the power industry has been subjected to an increasing number of cyberattack attempts. Beginning in the 1980s, about 800 cyberattacks have been observed in the energy sector [29].

### 2.1. History of Cyberattacks

In recent years, several cyberattacks have hit the control system of the electric power sector around the world [30]. In June 2007, a power outage lasting approximately 46 min in the Tempe area of Arizona affected about 100,000 customers, leading to a loss of 400 MW of load. The cause of the outage was due to the accidental activation of the load reduction program [29,31,32]. Similarly, in February 2008, a system disturbance in South Florida caused by a transmission system failure led to a loss of 2300 MW of load [29,31,32]. These two reported incidents were not considered intentional and malicious attacks; however, it shows the cyber vulnerabilities in the power system. In this context, the work in [32] presents a detailed survey and analysis to understand the motivation of the main cyberattacks that occurred between 2001 and 2013. In addition, this survey informs the attack targets and describes the techniques used by the attackers [32]. The identified main targets of cyberattacks were those directed at countries with national security risks; the country's strategic infrastructure, industries, and companies; global espionage; and the encouragement of hacker activity [32]. A historical analysis of the major cyber incidents that have occurred worldwide, with the first event dating back to 1903, is available in [33].

From these lists, it is possible to infer how these attacks occurred, identify possible vulnerabilities, and observe an increasing number of attacks in recent years and the greater complexity and refinement in cyber invasions. In 2010, the control facilities of the nuclear power plant in Iran were attacked by a computer worm called Stuxnet [33–35]. This malware is dangerous because it self-replicates, spreads throughout the system, and exploits unpatched vulnerabilities in the operating system of process computers [33]. Stuxnet is considered one of the main cyberattacks described in the literature, as it has caused changes in countries' cybersecurity strategies and policies [33,35]. A recent example of the devastating effects of cyberattacks occurred on December 2015, in the Ukraine, where 225,000 consumers lost their energy supply for a few hours due to a forced blackout [32,34,36–38]. This event became known as the worst power system blackout caused by a cyberattack ever recorded in the literature [32,34,36,37].

The healthcare sector, universities, research centers, hospitals, and laboratories during the coronavirus disease pandemic (COVID-19) suffered a coordinated set of cyberattacks on their information and communication system. These attacks aimed to extract unauthorized information from the development of vaccines and drugs that combat COVID-19. In March 2020, a university hospital in the Czech Republic suffered a cyberattack that disrupted its Internet network and caused delays and postponements of surgeries and emergency care [39]. Nine other cyberattacks and breaches in the healthcare sector during the COVID-19 pandemic are presented in more detail in [39]. Table 1 presents a historical perspective of critical cyberattacks on industrial control systems and the power and energy sector.

In addition to cyberattacks, the power grid is also subject to cyber-terrorism actions focusing on spreading fear to the population under service [40,41]. In this new form of terrorism, Pakistan stands out with the largest number of attacks (439), followed by Yemen (170), Colombia (161), and Iraq (146). Figure 2 shows the number of terrorist attacks that the electricity sector of selected countries experienced between 2010 and 2014 [40,41].

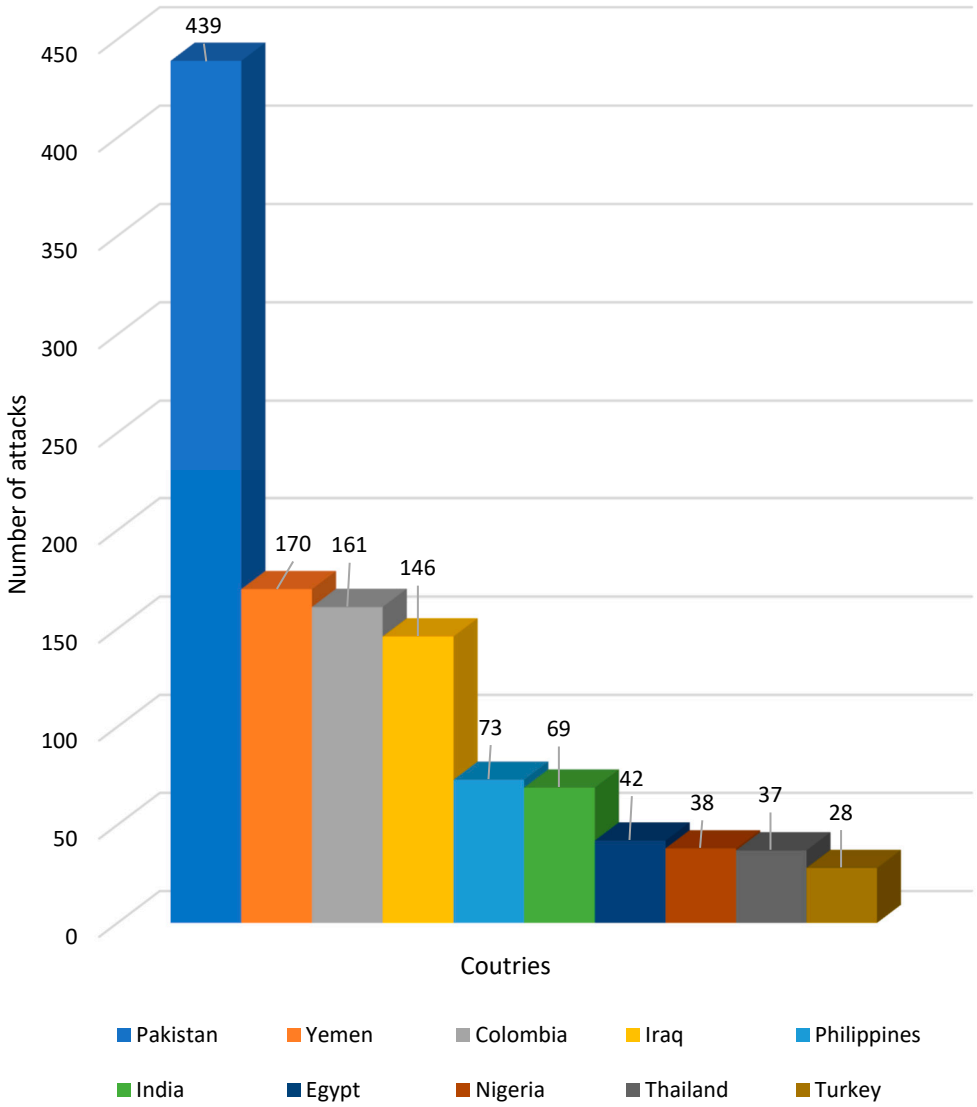


**Figure 2.** Number of terrorist attacks in the electricity sector of selected countries [40,41].

**Table 1.** Cyberattacks in industrial control systems and the power and energy sector [33,34,38,42–45].

| Year | Involved Countries | Type of Cyberattack | Cyber Incident |
|---|---|---|---|
| 1982 | URSS | Code manipulation | Pipeline destruction in Siberia due to manipulation of control software code causes valves to malfunction [38]. |
| 1999 | Bellingham, USA | Code manipulation | Code manipulation that led to a slowdown of a pipeline SCADA system [38]. |
| 2000 | Queensland, Australia | Attack | Cyberattack on Maroochy Water Services. This wireless attack remotely controlled 150 pumping stations and released millions of gallons of untreated sewage [33]. |
| 2003 | Ohio, USA | Malware | The Ohio nuclear power plant suffers the injection of a Malware (Slammer Worm) into its control system [34,38]. |
| 2007 | Idaho National Laboratory, USA | Attack | A hacker injected false data and controlled a generator breaker. This cyberattack became known as the Aurora Attack [34,38]. |
| 2008 | Turkey | Attack | Explosion of oil and barrels in Turkish pipelines caused by false data injection attacks that manipulated the control system [34,38]. |

**Table 1.** *Cont.*

| Year | Involved Countries | Type of Cyberattack | Cyber Incident |
|---|---|---|---|
| 2010 | Iran | Malware | Iran's nuclear power plant control facilities were attacked by a malware called Stuxnet [33]. |
| 2010 | China, USA, and Netherlands | Malware | Night Dragon malware: This cyberattack was targeted at large companies in the energy and oil sector [33]. |
| 2011 | Global | Malware | Duqu/Flame/Gauss malware: This malware was discovered by Hungarian researchers in 2011 and aims to steal information from the control system of companies and their suppliers [33]. |
| 2012 | Global | Campaign (series of attacks) | In 2012, a set of cyberattacks targeting the oil and natural gas industry was discovered. This series of attacks is called the Gas Pipeline Cyber Invasion Campaign [33]. |
| 2012 | Saudi Arabia and Qatar | Malware | Power generation and supply has been affected due to this malware attack on the computer system of large energy companies in the Middle East. This attack is known as Shamoon Malware [33,34,38]. |
| 2013 | USA and Russia | Attack | In 2013, the attackers carried out a cyberattack on a company that provides maintenance services on a store's air-conditioning, heating, and ventilation system. From this attack, the hacker was able to extract financial data from the target stores. This cyber event became known as Target Stores Attacks [33]. |
| 2013 | USA and Iran | Attack | The Bowman Dam that controls the water level after abnormal storms was accessed by Iranian invaders through a cyberattack, according to the US. This cyber event became known as the New York Dam Attack [33]. |
| 2013 | USA and Russia | Malware | The Havex malware is a trojan horse that has the ability to remotely access and collect unauthorized information from industrial control systems [33]. |
| 2014 | Germany | Attack | A steel mill in Germany suffered a cyberattack based on spear-phishing and social engineering. The attackers gained access to the industrial control system and caused several failures in the control, operation, and triggering of equipment [33]. |
| 2014 | Global | Malware | BlackEnergy malware is a cyberattack that aims to extract information from the various Human–Machine Interface providers [33]. |
| 2014 | USA, Turkey, Switzerland, and Russia | Campaign (series of attacks) | The energy sector in the USA, Turkey, and Switzerland suffered a campaign of cyberattacks aimed at spying and accessing confidential information from the control process. This cyber incident became known as Dragonfly/Energetic Bear Campaign No. 1 [33]. |
| 2015 | Ukraine | Attack | In 2015, the blackout in Ukraine was caused by the injection of false data into the power grid. This cyber event affected thousands of users for a few hours and was considered the first successful attack on a country's power system [33,34,38,42]. |
| 2016 | Syria and USA | Attack | A water treatment company suffered a cyberattack on its control system that modified the dosage of chemicals used in its processing. This cyberattack became known as the Kemuri Water Company Attack [33]. |
| 2016 | Saudi Arabia and other Middle Eastern countries | Malware | After four years, the Shamoon malware was used again for a cyberattack on the computer system of the civil aviation sector in Saudi Arabia and other Middle Eastern countries. This attack aimed to erase data from the system [33]. |

**Table 1.** *Cont.*

| Year | Involved Countries | Type of Cyberattack | Cyber Incident |
|---|---|---|---|
| 2016 | Ukraine | Attack | The Ukrainian power grid once again suffered a cyberattack that led to power outages. This time, this attack was more robust, and a denial-of-service attack hit the telephone system. The new malware used in this attack is known as Crashoverride [33,42]. |
| 2017 | USA and Ukraine | Malware | CRASHOVERRIDE is malware responsible for generating power interruptions in countries' power systems. The cyberattack in the Ukraine in 2019 used this mechanism [33]. |
| 2017 | Iran, USA, Saudi Arabia, and South Korea | Group (set of malwares) | APT33 is a set of malwares that aims to spy on the aviation, energy, and petrochemical industries. In addition, this cyberattack has the destructive ability to erase process data and share confidential information with attackers [33]. |
| 2017 | Ukraine, Russia, USA, UK, and Australia | Attack | NotPetya is malware that was initially used against the Ukraine and has the ability to target a nation's critical infrastructure. It is a destructive cyberattack of Russian origin [33]. |
| 2017 | USA | Campaign (series of attacks) | Dragonfly/Energetic Bear No. 2 is a set of cyberattacks that target a country's strategic infrastructure sectors, such as the electric and nuclear power grids and the water supply [33]. |
| 2017 | Middle Eastern countries | Malware | TRITON/Trisis/HatMan consists of new malware that has the ability to access and modify confidential information and execute algorithms that destabilize the industrial security system [33]. |
| 2019 | USA | Attack | A cyberattack interfered with power grid operations in the US on 5 March 2019. The type of attack used was denial of service. This was the first cyberattack in the wind and solar energy sector [34]. |
| 2019 | India | Malware | The Kudankulam nuclear power plant in India suffered a cyberattack in 2019 [34]. |
| 2019 | Venezuela | Attack | In 2019, the power grid in Venezuela was attacked, causing a power outage for more than five days in several states, including the capital [42,43]. |
| 2020 | Portugal | Ransomware (malware) | The giant Portuguese energy company, Energies of Portugal, was attacked in 2020 by Ragnar Locker. The attackers reportedly stole 10 TB of confidential data [43]. |
| 2020 | Brazil | Attack | On 16 June 2020, a Brazilian power generation and distribution company, Light S.A., was attacked by a Sodinokibi malware and had its operation temporarily halted [43]. |
| 2020 | Venezuela | Attack | In 2020, the power grid in Venezuela was attacked, causing a power outage in several states, except the capital [44]. |
| 2021 | USA | Ransomware (malware) | A set of hackers used the ransomware attack and broke into Colonial Pipeline's network and digital systems, leading to an outage of the pipeline for several days [45]. |

### *2.2. Classification of Cyberattacks*

Smart microgrids are a major target of cyberattacks that can be typically clustered into three distinct types of attack classification [31,46–51]:

(i). Availability;
(ii). Integrity;
(iii). Confidentiality.

This section seeks to provide a general overview and description of the main types of cyberattacks currently identified in the literature, Figure 3. The reader interested in a detailed analysis for each cyberattack is kindly referred to the reference works cited in each subsection.

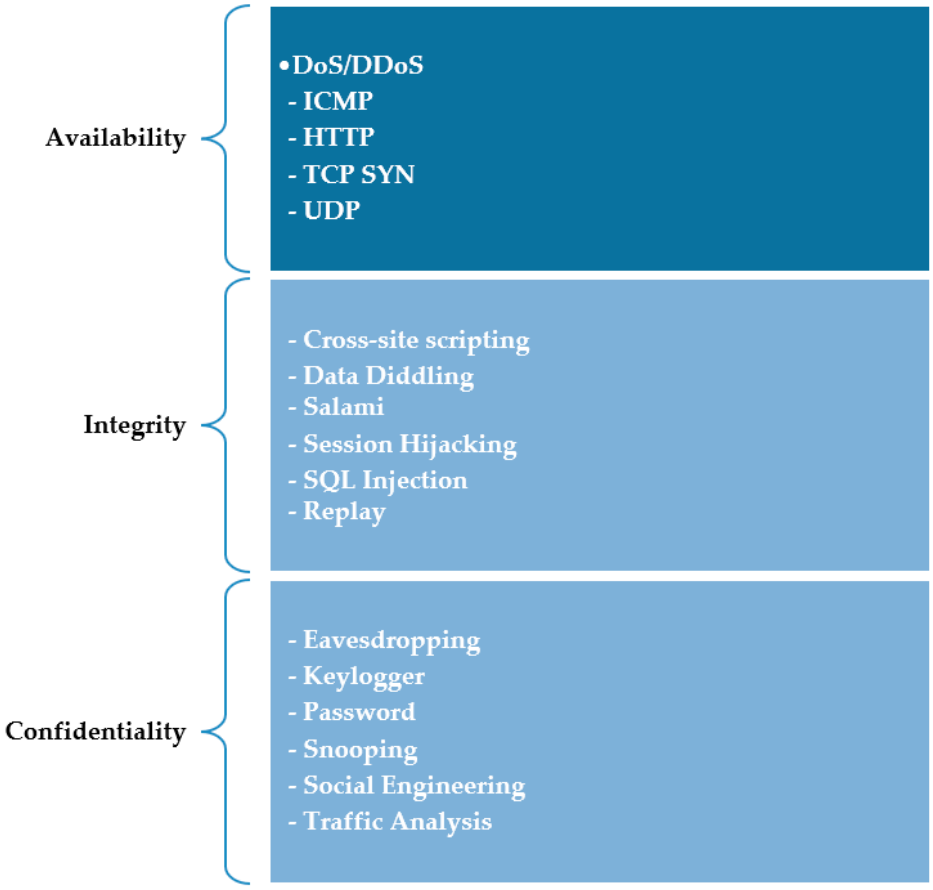


**Figure 3.** Classification of cyberattack [50,51].

#### 2.2.1. Availability

Real-time data of power grids must be readily available for access and consultation with system operators and automated control systems. Ensuring this data security is necessary because catastrophic consequences such as brownouts and blackouts can occur based on its tampering and/or lack of availability. In this sense, cyberattacks focused on data availability happen when malicious information is sent, causing network or server congestion. Consequently, an interruption or delay of data communications occurs. This event is called a data availability attack [31,46–51]. The next sections describe the main attacks against data availability.

##### A. DoS/DDoS

Denial-of-service (DoS) attacks aim to overload the network and block system communication to interrupt the user's request for service. One way to carry out these attacks is to intentionally send many messages on the control channel to congest the network and obstruct communication. The attacker can carry out the attacks directly by using one's personal computer or indirectly through bots (the hacked system that is under the control of the attacker), or both [50]. Furthermore, these attacks are dangerous and cause considerable losses [50,52–54].

A variant of DoS attacks is denoted as a distributed denial-of-service (DDoS) attack. A DDoS consists of a distributed attack coordinated by an attacker who acts as the "Attacker-in-Chief" or several bots that attack the target and make the network resources unavailable

to the user [50,52–57]. The DDoS attack is considered one of the most destructive network attacks [56]. The attacker follows four steps to begin the attack [57]:

- It studies the system information to find possible vulnerabilities in the network and then sends an attack;
- The attacker creates bots that install malicious programs on the invaded computers so that they can be controlled. The hacked computers are called zombies;
- The attacker encourages the invaded computers to send various attack messages to target the victim;
- The attacker extracts the information of interest and erases the data from memory.
- The main consequences of DoS/DDoS attacks are as follows [50,56]:
- Communication network slowness;
- Blocking authorized users' access to system resources.

The following describes some types of DoS/DDoS attacks.

A1. ICMP

The Internet Control Message Protocol (ICMP) is the protocol responsible for reporting errors to clients while delivering Internet Protocol (IP) packets. This protocol acts at the network layer of the TCP/IP (transmission control protocol) model. The attacker generates and sends numerous ICMP requests, congests the information traffic, and exploits the bandwidth of the victim's system [50,54,58]. There are two ways for ICMP to occur: the "ping of death attack" and the "smurf attack" [50].

A2. HTTP

The Hypertext Transfer Protocol (HTTP) is the protocol responsible for transferring hyperlinks and is the basis of data communication on the web. This protocol acts at the application layer of the TCP/IP model. The target of these attacks receives numerous GET and POST messages in order to overload, congest, interrupt, and confuse the traffic of truthful information and the communication of web applications that use the HTTP protocol [50,59]. In contrast to the ICMP attack, the HTTP attack does not exploit system bandwidth significantly, since a high number of requests is not required [50,59].

A3. TCP SYN

The TCP SYN attack consumes system memory and makes the user's access to services unavailable. Furthermore, it uses an imperfection in the TCP protocol to perform the invasion. The communication process takes place in a "three-way handshake" format. There are three steps in this process. In the first step, the user sends the "synchronization" (SYN) request to the network server. Then, to authorize the communication, the server sends an acknowledgment (ACK) and returns the SYN request to the user. In the last step, in theory, the client should send an ACK message to confirm and acknowledge the communication. However, this message does not reach the server. In this last step, the attacker is sending numerous fake SYN messages, and by not providing the ACK, it generates a communication failure and network overload [50,54,60].

A4.UDP

The user datagram protocol (UDP) is a protocol that acts at the transport layer of the TCP/IP model. In addition, it has the characteristic of being a connectionless protocol. In this type of attack, the attacker creates and sends many packets with fake addresses to increase network traffic. In this way, it floods the system bandwidth. The server cannot check and respond to requests correctly and starts to crash. This attack implies the unavailability of system services for authorized users. The attacker may have a specific target or a totally random port [50,54,57,61,62].

2.2.2. Integrity

For adequate functioning and control of power grids, it is necessary that the data present accuracy, coherence, and veracity. Attacks happen when some command signal or the periodic

measurements are altered, damaging the integrity of the data [31,46–48,50,51]. False Data Injection (FDI) is an example of an attack focused on affecting data integrity [48,49]. In the following, key attack strategies focused on compromising data integrity are presented.

A. Cross-Site Scripting

Cross-Site Scripting (XSS) attack is an important type of code injection attack (CIA) and one of the most common. This attack exploits the system's security weaknesses by executing an invalid code. The attacker creates the malicious code and propagates it through the web browser. When the victim accesses the infected site, the attacker can access the system's sensitive information [50,63–65]. Thus, the integrity of the victim's data is in danger since the system has been hacked. The XSS attack can happen persistently, non-persistently, or through a "document object model" (DOM) [65].

B. Data Diddling

Data Diddling Attacks consist of an attack that modifies the information in the database without authorization, which is illegal. In addition, the attack can change the status of files from permanent to temporary or from private to public, among other inappropriate changes that damage the integrity of the information [50,66].

C. Salami

Salami Attacks consist of performing small attacks on the network data system to extract an adequate amount of sensitive information without being noticed by the security system. These attacks provide a larger attack and, consequently, larger damage to the company [50,66].

D. Session Hijacking

A Session Hijacking attack is the misuse of a part of the network, causing the attacker to become a participant with access to the information on that part of the system. The attacker can send false information packets to other users as if the attacker was one of the network administrators. The hijacker seeks to find and exploit the weaknesses and unencrypted protocols of the network [50,67].

E. SQL Injection

The SQL Injection Attack, like the XSS attack, is an important type of code injection attack and one of the most common. The attacker seeks to use weaknesses in SQL statements to access database information. This attack happens when the hacker uses an improper SQL command that provides access to a website's database. With this improper entry, the attacker can access all the victim's information in this database and delete, modify, download, or do any other improper activity [50,63,68]. Tautologies, Arbitrary String Patterns, Group Concatenate String, Stored Procedures, and Alternate Encoding are some types of SQL injection attacks [63].

F. Replay

A replay attack (RA) is a form of cyberattack that aims to compromise the integrity of the information of the system components. This attack aims to monitor and record a real sequence of sensor measurements and, during the invasion, replace the real measurements with these previously recorded values. These recorded data are replayed and repeated uninterruptedly until the end of the attack. Therefore, the replay attack takes place in two stages, the monitoring stage and the replaying stage. This fraudulent replay attack does not require deep system knowledge and usually targets and affects the operation of the sensors, actuators, controllers, and estimators of the cyber–physical system [36,69].

#### 2.2.3. Confidentiality

Sensitive system information should only be accessed by authorized individuals to ensure data confidentiality. Thus, when unauthorized individuals access the system planning, the control, operating strategies, and user information are no longer secure. Therefore, it

is subject to espionage and misuse by third parties. Thus, attacks on data confidentiality can affect the functioning of the system and also cause financial and physical/technical impacts [31,46–48,50,51].

A. Eavesdropping

The process of secretly listening in on the network to unauthorized conversations is called eavesdropping. The eavesdropper has access to privileged and confidential information among network users. In this way, the eavesdropper can read, insert false information into the network, and delete or do any illicit activity with the system data [50,70]. Therefore, with this attack, the confidentiality of communication is damaged.

B. Keylogger

Keylogger consists of a malicious software program that is installed on the system without the knowledge and authorization of the client. It is intended to monitor and capture the user's activities intentionally. Subsequently, attackers have access to this confidential data and can steal from, harm, or exploit the victims [50,71–73]. Keyloggers can be implemented using hardware or, more usually, software, wireless, and acoustic [72,73]. A credit card machine that records and then makes the password available to others is an example of a keylogger [71]. Therefore, this type of attack compromises the secrecy of information.

C. Password Attacks

The simplest and cheapest way to initially protect the information systems of a user, a company, or the government is through authentication using passwords [74]. However, this method presents some vulnerabilities because the user can create a password considered weak, reuse the same password on several sites, access unreliable sites, type passwords on unreliable computers, and other actions that compromise the confidentiality of passwords and, consequently, facilitate the action of hackers [74,75]. There are numerous ways for the attacker to discover the user's password. In this context, we can highlight the following [50]:

- Attack based on the combination of all characters contained in the dictionary;
- Attack using hacking software that tries numerous possible password combinations,
- Guessing attack, the attacker uses the victim's personal data to discover the password.

The discovery of the password by a third party can lead to leaks and theft of sensitive information, economic losses, invasion of privacy, and other catastrophic consequences for the user.

Changing passwords periodically is a simple way to defend password integrity [76]. Generally, passwords created by the user him/herself and which are memorable are easier to crack by attackers. Thus, some tips for creating a strong and unique password using mnemonic passwords are given below [75,77]:

- Sentence substitution: Choose a sentence and substitute each word or digit with other characters;
- Keyboard change: Choose a basic password and then add characters according to the random movement chosen by the user. You must save this movement;
- Use the formula: Put the password in the format of an equation or function with numbers and characters,
- Special character insertion: Replace conventional characters in the basic password with special characters.

D. Snooping

Snooping is a cyberattack that has the passive characteristic where the attacker seeks to obtain sensitive information from users [50,78]. Snooping can happen in a direct way where the attacker unnoticed watches the victim enter his password or any other confidential information. In this way, making a physical attack. Snooping can also be performed online, where the hacker monitors the target via the Internet in order to obtain network data, company confidential information, and passwords from the victim. In addition, this attack

can happen by hacking into security cameras, switches, and routers on the network, thus making it a digital attack [50].

E. Social Engineering

Social Engineering consists of a cyberattack that aims to target the individual rather than the network structure of the system [79]. This attack uses persuasion techniques to trick and manipulate victims until they reveal confidential information that benefits the attacker [50,79,80].

Nowadays, due to the use of social networks, individuals share personal information for free, and this fact helps criminals to profile each person and then perform a Social Engineering attack [79]. In this way, phone calls, email exchanges, social networks, and conventional websites are all used as objects for attacks [79,81].

Phishing; Grooming; Pretexting; Profile Cloning; Face-to-Face Interaction; Shoulder Surfing; Quid Pro Quo Attacks; Diversion Theft Attacks; Piggybacking or Tailgating or Trailing and Pretending; File Masquerade; Baiting; Reverse Social Engineering; Scareware or Pop-Up Windows; and Water-Holing are some types of social engineering [81].

F. Traffic Analysis

The Traffic Analysis attack is a cyberattack where the attacker performs a previous analysis of the communication traffic between the sender and receiver. It aims to extract confidential information to learn about the network's vulnerabilities. Subsequently, it carries out the planning for the execution of the theft. This attack has a passive characteristic and hurts the confidentiality and privacy of the users' information [50,52].

## 3. Cyber–Physical System

Technological advances in industries drive the emergence of cyber–physical systems [82,83]. Figure 4 illustrates the CPS system in a block diagram. This type of system integrates the physical aspects of a process and digital technology [84,85]. In addition, using computational concepts, the CPS can act and expand the components on the shop floor, being an important factor in the technology development [84]. The CPS develops a leading role in the development of the industrial Internet of Things (IIoT) and Industry 4.0 [86]. This evolution in the industry provides better access to the information provided by sensors and, consequently, impacts the generation of a high number of data continuously, the so-called big data [87]. In this way, the CPS provides a precise and real-time operation [82,86,88]. Currently, the CPS is the object of study in the literature, since it impacts the economy, environment, and people's daily lives. In this context, the work developed in [89] presents a review of the literature on CPS applications in 10 research fields: agriculture, education, energy management, environmental monitoring, medical devices and systems, process control, security, smart city and smart home, smart manufacturing, and transportation systems.

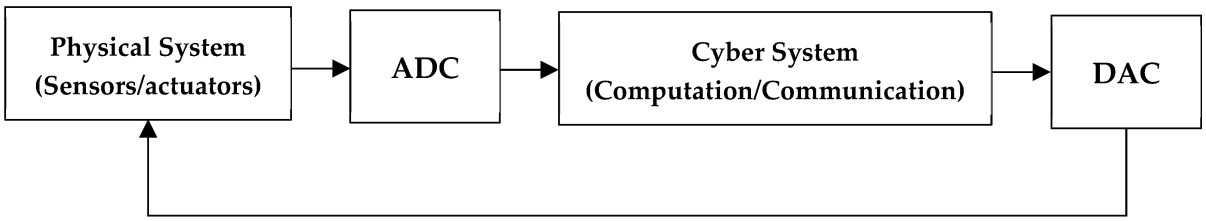


**Figure 4.** Block diagram of a cyber–physical system.

The following sections display the architecture layers and basic components of a CPS.

### *3.1. Cyber–Physical System Layers*

The architecture of a CPS is divided into three main typical layers: perception layer, transport layer, and the application layer. Figure 5 illustrates the architecture of a CPS from

the layers' point of view. In the following, the characteristics of each layer are presented and discussed.

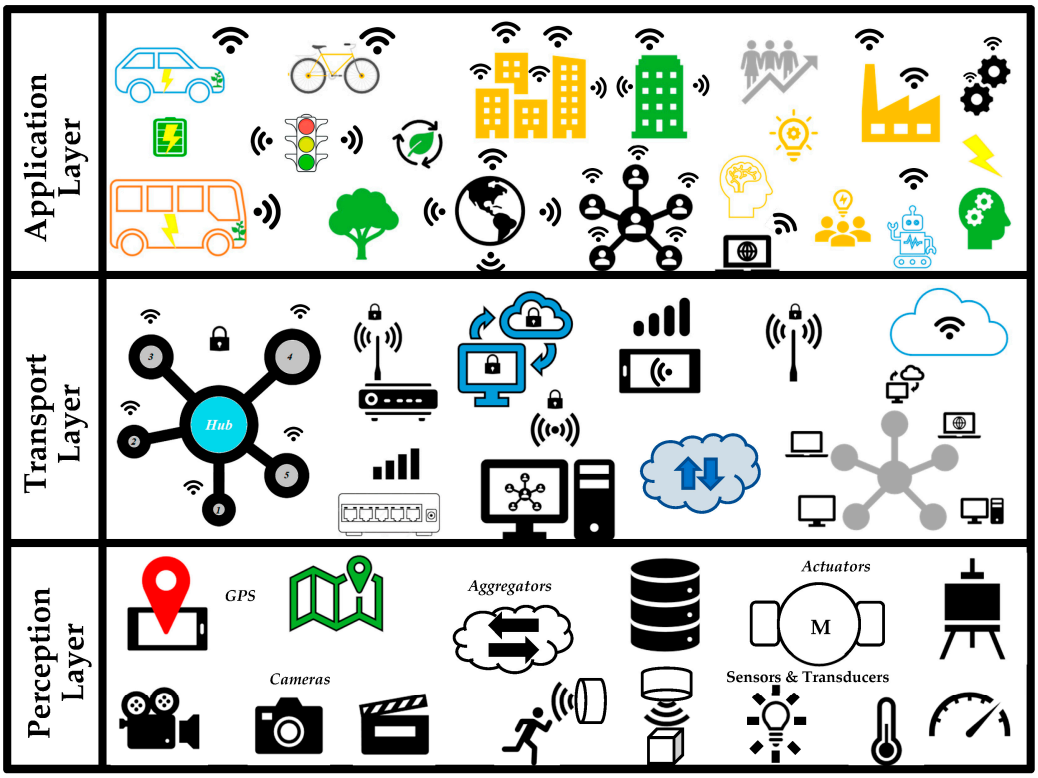


**Figure 5.** Cyber–physical system layers' representation.

#### 3.1.1. Perception Layer

The first layer of the CPS architecture is called the perception layer. This layer holds all the equipment that will interpret the physical phenomena and transform them into electrical signals and, subsequently, into information. Some equipment of this first layer is aggregators, actuators, sensors, transducers, Global Position System (GPS), cameras, "Radio-Frequency Identification" (RFID) tags, lasers, and any other intelligent equipment of the so-called "factory floor" [86,90]. This layer aims to collect real-time process information to perform planning, monitoring, and control of the physical system. Due to these factors, in the literature, this layer is also known as the "sensing layer" and "recognition layer" [56,90].

#### 3.1.2. Transport Layer

The second layer of the CPS architecture is called the transport layer. This is the intermediate layer between perception layer and application layer, thus being responsible for the communication of data between the layers. This seamless communication is accomplished through wired or Wi-Fi Internet networks, Bluetooth technology, Infrared (IR), 4G and 5G, Zigbee, and Internet protocols, among other technologies that aid communication. In addition, this layer is responsible for routing and transporting data through routers, switches, hubs, gateways, and clouds. In the literature, the intermediate layer is also known as the transmission layer or network layer [56,90].

#### 3.1.3. Application Layer

The last and most interactive layer of the CPS architecture is called the application layer. The role of this layer is to receive information from the transport layer, analyze it and send appropriate command signals to the devices located in the perception layer to act in the physical process. The application layer uses intelligent decision-making algorithms to analyze the information received and, consequently, make the most appropriate control

decision for the proper functioning of the physical system [91]. In addition, system monitoring is performed in this layer, seeking to map the behavior of the physical system to assist in the decision-making process. Furthermore, the application layer can save previous decision-making from obtaining operational improvements and future feedback [86,90].

### *3.2. Cyber–Physical System Components*

The components that make up a CPS are divided into three groups:

(i). Physical components;
(ii). Detection components,
(iii). Control and communication components.

#### 3.2.1. Physical Components

The physical components of a CPS are sets of equipment that enable the operation of the physical process. The major components of a Cyber–physical Power System (CPPS) are the power generators, transformers, switchgear, transmission line, circuit breakers, motors, cylinders, and numerous other loads that describe the power system [92].

#### 3.2.2. Detection Components

The sensing components are devices that are physically connected to the physical system and are responsible for observing and extracting information from the process. This unit highlights three types: sensors, aggregators, and actuators.

- Sensors

These devices are in the perception layer and are connected directly to the physical system components. The sensors are responsible for interpreting the physical phenomenon and transforming it into a signal that can be interpreted. In addition, they have the function of collecting the information from the physical system and through the aggregators sending it to the transport layer [86,93].

- Aggregators

These are devices that are mostly located in the transport layer and responsible for processing the data received by the sensors. It works as a "bridge" that transports the data obtained by the sensors, from the perception layer to the transport layer. Online data aggregators are found in routers, switches, gateways, and other devices performing this transport function [86,93].

- Actuators

These are devices located in the application layer. Actuators receive a message indicating their operation based on data processing and decision-making from the aggregators. In addition, they are responsible for modifying system parameters so that the process operates properly. Actuators receive messages in the form of electrical signals and hydraulic or pneumatic energy and generate physical actions as responses [86,93]. Motors, valves, and cylinders are examples of actuators.

#### 3.2.3. Control and Communication Components

The control and communication components of a CPS are devices responsible for monitoring and managing the physical system. In addition, they seek to control the process to achieve z satisfactory performance, reliability, and security. Therefore, control devices are fundamental for the robustness of the system. In this perspective, Programmable Logic Controllers (PLCs), Distributed Control Systems (DCSs), and Remote Terminal Units (RTUs) are elements that stand out to control, and the Supervisory Control and Data Acquisition (SCADA) and Phasor Measurement Unit (PMU) perform the data acquisition in a CPS system. The following sections detailed describe these components.

- Programmable Logic Controllers (PLCs)

PLCs are digital computers that, through user programming, can automate and control modern industrial processes. Initially, these devices were developed to replace industrial relay panels and emulate the behavior of electrical diagrams. Besides that, this device presents characteristics that facilitate fault diagnosis, good flexibility, resistance to vibrations, immunity to electrical noise, support algorithms and loops, easy programming, low cost, robustness, and good reliability, among other important aspects [86,94]. The basic building blocks that make up the PLC hardware are a rack, a power supply, a programming unit, input and output (I/O) modules, and the central processing unit (CPU) [95]. Thus, the PLC is used for various industrial control and automation applications, from simple to more complex systems [95].

- Distributed Control Systems (DCSs)

Centralized control for large and complex systems may present a different efficiency, reliability, controllability, flexibility, and robustness as communication failures [96]. From this perspective, physical system processes are divided into subsystems and locally controlled through industrial computers, thus allowing the distribution of control and greater flexibility in operator action [86,96]. In addition, monitoring can be performed through supervisory systems that provide online and remote control. In this way, DCSs have reduced implementation costs while increasing the reliability and robustness of the system [86].

- Remote Terminal Units (RTUs)

RTUs are electronic devices that extract the signal samples, investigate, and identify possible failures and then restore the data in a distribution system [97]. In comparison with PLC, the RTU does not perform well in algorithms and control loops, as well it presents low immunity to vibrations and noise [86]. Its main application is focused on geographical telemetry systems, being used to extract information from the system, send/receive messages, and perform control actions in a SCADA system [98], while presenting some processing capacity due to its microprocessor unit [86]. In addition, some RTUs can also control numerous systems that are connected to the control room [99].

- Supervisory Control and Data Acquisition (SCADA)

These systems use software to collect, measure, monitor, process, and control the data and equipment in a CPS [100]. The SCADA system extracts and processes the data generated by the PLCs and RTUs [101]. The typical SCADA system architecture features a "Human–Machine Interface" (HMI), hardware, software, RTU, central supervisor, database, measurement devices, and process actuation [100,102]. These systems' communication networks can be based on Internet protocols, providing benefits in monitoring, planning, management, and control of the CPS. However, this can also bring some harm, such as a higher number of cyberattacks on the vulnerabilities of the SCADA system [103].

- Phasor Measurement Unit (PMU)

PMU technology is used in power systems to measure a "quantity" called a phasor. The phasor is a graphical representation of the magnitude and phase angle of an alternating current electrical quantity at a specific time. In this way, it aims to improve the precision of the visualization of electrical quantities at all points of the network and, therefore, facilitate the diagnosis of possible failures in the system [104,105]. Using GPS for the time-stamping of samples, PMUs can measure the frequency and the rate of change of the frequency of electrical signals. For this reason, they are also known as synchrophasors [106]. Systems with PMUs have a higher update rate and accuracy of around $1\ \mu s$ compared to SCADA systems [107,108]. From this perspective, using data acquisition with PMU technology provides real-time measurement, analysis, and control of system dynamics that cannot be achieved using a traditional SCADA system.

### *3.3. Cyber–Physical System Vulnerabilities*

The current integration between people and machines controlled remotely in real-time by Internet networks, data processing, and new computer and information technologies

provide benefits regarding the efficiency and performance of the control system in industries and in the automation of processes. In counterpart, this system presents new evils concerning the cybersecurity of information on physical devices, communication, monitoring, operation, and control of the cyber–physical system.

From this perspective, the cyber–physical system presents new weaknesses in its operation that are known as cyber, physical, and cyber–physical vulnerabilities. The cyber vulnerability relates to the network system, communications, smart devices, remote access, and unintentional failure of employees and vendors [109]. The physical vulnerability is related to physical attacks on the devices that make up the infrastructure of the cyber–physical system, such as the sensors, transducers, actuators, motors, cylinders, pumps, valves, transmission line cables, and distribution and transmission transformer towers, among other physical devices that make up an industrial system [109]. Finally, there is the cyber–physical vulnerability which represents a new type of vulnerability that is concerned with the weaknesses and damage presented by the junction of cyber and physical devices and components of the critical infrastructure of an industrial cyber–physical system [109].

Modern systems of monitoring, control, and industrial management are performed by SCADA systems or other industrial control systems that use as a primary element a set of systems with PLCs [110,111]. PLCs, through their inputs, are responsible for receiving and processing the data received by sensors and transducers connected to the industrial process, and through a programming logic and signal issued, they can determine how the actuators, motors, frequency inverters, relays, transformers, and other final control elements will work in the industrial process [110]. From this perspective, the PLC integration with new Internet technologies makes it a target of cyberattacks on its communication network, such as Stuxnet [111], Triton, and Black Energy [112], and consequently, such devices present a vulnerability in cybersecurity and are part of the critical infrastructure of the industrial control system of a CPS.

PLCs are connected to and integrated into the Internet of Things; therefore, they are vulnerable to malicious threats in their control logic. This type of attack is called control logic injection, and it aims to cause failures and disruptions in the processes controlled by PLCs. In this perspective, the author of [112] presents recent work on control logic injection attacks and points out the recommendations and current challenges in the security and protection of information in PLC-controlled systems. Besides the control logic injection attack, there is the denial-of-service attack, wherein a large number of malicious packets are sent and transmitted that exploit the possible security vulnerabilities of a PLC system [113]. Thus, the author of [113] discusses a methodology capable of detecting anomalies based on monitoring the behavior of the CPU of a PLC in a water tank control system.

Cybersecurity in management and control systems with PLCs is important to maintain the availability, integrity, and confidentiality of process data and ensure proper and resilient operation of the industrial system. Thus, the author of [114] presents a study that points out the challenges in information security and discusses the security of communication protocols in Industry 4.0 systems that use PLCs and SCADA. The author of [111] takes a different approach than the conventional one, considering the communication network between engineering stations and PLCs as an object of study and analysis of cybersecurity.

## 4. Cybersecurity Applications and Methodology

We followed a methodological approach based on the strategy proposed in the Introduction, and this section presents the state-of-art of cybersecurity applications based on multiple scholarly and industrial database resources, including but not limited to Science Direct, IEEE Xplore, Google Scholar, and MDPI databases, among others. The literature search on cybersecurity applications is divided into three main categories: cybersecurity on monitoring systems, cybersecurity in control systems, and cybersecurity in protection systems, as shown in the Figure 6. Thus, the subsections below are meant to provide the available references of each topic of interest.

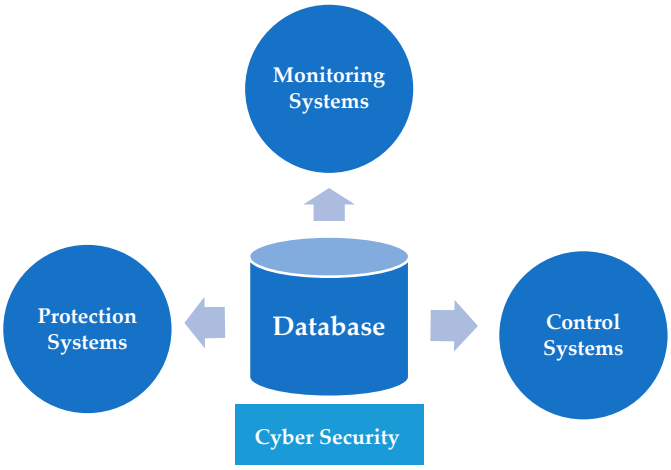


**Figure 6.** Literature search on cybersecurity applications.

### *4.1. Cybersecurity on Monitoring Systems*

The cybersecurity of the monitoring system of a CPS is extremely important because it considers the security of the information collected by sensors and measurement instruments. Therefore, for this process to achieve satisfactory results, the monitoring system must present information security and reliability. In this category, 10 key works were selected and are shown in Table 2.

**Table 2.** Cybersecurity applications: monitoring systems [115–124].

| Method | Attack Point | Purpose | Field of Application | Simulation | Reference |
|---|---|---|---|---|---|
| Multilayer Run-Time Security Monitor | Application and communication layer attacks. | Identify divergences caused by communications and application layer attacks and prevent propagation to other control layers. | ICPSs | Water distribution system. | [115] |
| Regularized sparse deep belief network (RSDBN) model is adopted; noise-adaptive Kalman filter | Hierarchically distributed attack in ICPS layers, perception, and application layer. | Identify potential cyberattacks through hierarchically distributed intrusion detection. | ICPSs | Numerical simulation on an ICPS platform with OPNET and benchmark simplified Tennessee Eastman process | [116] |
| Three unsupervised machine-learning algorithms: OCSVMs, LOF, and AEs | Network scanning, denial of service, and malicious command data injection. | Detection of cyber and physical anomalies. | Critical infrastructure of the CPS | IEEE-33 bus model | [117] |
| Machine-learning algorithms | Critical Infrastructure Attack | Cyber and physical anomaly detection | Critical infrastructure of the CPS | Power plant | [118] |
| Multicriteria decision-making (MCDM), Choquet Integral in compute CP-SAM | Malicious and accidental microgrid failures | Increase the resiliency, reliability, and security of a microgrid by creating a robust cybersecurity assessment metric. | Cyber–power system | The test was performed using a real microgrid model | [119] |

**Table 2.** *Cont.*

| Method | Attack Point | Purpose | Field of Application | Simulation | Reference |
|---|---|---|---|---|---|
| Big data platform architecture for log analysis for CPS and prediction algorithm based on time series | Log anomalies | Propose and implement a log analysis architecture capable of identifying and detecting anomalies in the power system. | Hydropower generation control networks | The tests were run with a real dataset from a CPS recorded over 3 months | [120] |
| Fuzzy hesitant methodology of the Analytic Hierarchy Process (AHP) and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) | On data availability, integrity, and confidentiality. | Analyze and estimate assessments through an operational procedure for the cybersecurity of the industrial system. | Industrial control system in the energy sector | Computational simulation of six different alternatives | [121] |
| Blockchain Technology | Malicious attack of false data injection into PLC. | Accurately monitor data and protect the PLC against cyberattacks. In addition, a system is proposed to ensure the operation of the Reactor Protection System. | Isolated networks of nuclear power plants | The proposed approach is tested through an experiment that injects dummy data into PLCs | [122] |
| AI algorithms | Real-time detection of anomalies in electrical appliances. | Data acquisition, fault identification, management, and real-time monitoring of energy data based on AI algorithms. | Industrial Internet of Things | Hardware design, server, and database creation in open source and computer simulation | [123] |
| Adaptive method and multicriteria optimization | Cyberattacks and network traffic anomaly detection. | Creating an adaptive system to manage and monitor information security. | CPS | Experimental study of intelligent home intrusion detection | [124] |

For monitoring industrial systems, industrial cyber–physical systems (ICPSs) are used, consisting of a link between the software and hardware parts of the system. Reference [115] developed a methodology called Multilayer Run-Time Security Monitor (ML-RSM), which is capable of identifying divergences caused by communications and attacks on the application layer, as well as preventing the spread to other control layers. The robustness of this approach is tested in a water distribution monitoring system [115]. To monitor and secure ICPSs, the author of [116] developed a robust tool capable of identifying possible cyberattacks through hierarchically distributed intrusion detection. Furthermore, through the adaptive Kalman filter, the monitoring and detection of possible anomalies in the CPS are performed [116].

To identify the interdependence of physical and cyber failures, the Reference [117] proposes an Anomaly Detection System (ADS). In this system, sensors collect data in the physical space and cyber sensors in real-time collect and analyze the network information. The methodology was tested on the IEEE-33 bus model, and three types of unsupervised machine algorithms were used for validation: one-class support vector machines (OCSVMs), Local Outlier Factor (LOF), and autoencoders (AEs) [117]. The critical infrastructures of the CPS are targets of cyberattacks, and in this context, the author of [118] proposes an anomaly detection methodology using machine-learning algorithms that relate physical and cyber–physical aspects to enhance the security of a power plant.

Resilience is an important characteristic of achieving reliability and security in a cyber–physical system. Thus, the author of [119] developed a technique to continuously measure and monitor it. This technique detects elements that undermine resilience and addresses probabilistic concepts, graph analysis, game theory, attack information, and CPS vulnerabilities [119]. The Cyber–Physical Security Assessment Metric (CP-SAM) has been tested and validated on a real MG model.

The monitoring of security risks in the power system is important to investigate the failures and identify the vulnerabilities of the CPS. In this context, Reference [120] proposes an architecture analysis to identify irregularities and a learning algorithm based on time series to predict abnormal network situations in the power system [120]. For estimating the cybersecurity of the power system, Reference [121] used the fuzzy hesitant methodology of the Analytic Hierarchy Process (AHP) and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). Furthermore, to verify the quality of the proposed methodology, the author tested six different projects [121].

The isolated networks of nuclear power plants (NPPs), e.g., PLC networks, are not immune to cyberattacks. Thus, the authors of [122] developed blockchain technology responsible for monitoring data accuracy and protecting the PLC from cyberattacks. Furthermore, a system is proposed to ensure the operation of the Reactor Protection System (RPS).

In the industrial sector, the use of the Industrial Internet of Things technology has seen continuous growth encompassing artificial intelligence (AI), computing, and cybersecurity. In this scenario, Reference [123] proposes an approach for data acquisition, fault identification, management, and real-time monitoring of energy data based on AI algorithms.

Information security in the monitoring layer of the CPS is important to maintain data integrity. In this sense, Reference [124] proposes an adaptive method that analyzes and solves a multicriteria optimization problem where the available inputs are mutable, seeking to ensure data integrity.

In Table 2, all the discussions mentioned above and research on cyberattacks on monitoring systems are analyzed and detailed.

Thus, the works discussed in this section present real-time defense strategies for protection against cyberattacks and in the detection of physical, cyber, and cyber–physical anomalies. The strategies are based on adaptive methods, Fuzzy Logic, AI and machine-learning algorithms, blockchain technology, prediction algorithms, and the Kalman filter. Therefore, these are important techniques found in the literature that seeks to improve the reliability, resilience, and cybersecurity of the devices that compose the monitoring system of a CPS.

### *4.2. Cybersecurity on Control Systems*

The cybersecurity of the Centralized or Distributed Control System of a CPS must be effective against cyberattacks from the simplest to the most complex form of systems. This is because the control system is responsible for correcting the process variables to achieve satisfactory operating parameters. Thus, for a process to achieve satisfactory results, the control system must be based on security and reliability information. The current power system presents a characteristic with distributed generation and devices interfaced with power electronics, generators, motors, and transformers connected in a grid. Thus, the cybersecurity of frequency and voltage control in these devices is a concern to ensure the transient and steady-state stability of the system. In this category, 10 key works were selected and are shown in Table 3.

**Table 3.** Cybersecurity applications: control systems [125–134].

| Method | Attack Point | Purpose | Field of Application | Simulation | Reference |
|---|---|---|---|---|---|
| Model Predictive Control | Cyberattacks of denial of service and fake data injection types | Develop a frequency control approach tolerant to cyberattacks. | Frequency Control of power systems. | The controller was tested on an IEEE benchmark system. | [125] |
| Adaptive control based on real-time CI (Computational intelligence). | Cyberattacks on the power system. | It presents a real-time testing methodology for analyzing and controlling power system stability and cybersecurity. | Power System | The test methodology was designed based on OPAL-RT and the SEL351S protection system. | [126] |
| Robust controller based on Port Controlled Hamiltonian with dissipation (PCHD) | False data injection attacks | A defense approach based on the energy conversion perspective. | Control system for a permanent-magnet synchronous motor. | The proposed approach is tested on an industrial CPS that controls a synchronous machine. | [127] |
| Long Short-Term Memory (LSTM) with Temporal Convolutional Neural Network (TCN) | False data injection attacks | A multivariate approach capable of accurately detecting the injection of false data into the CPS in real-time. | Smart Grid Control System | The performance of the designed framework is verified using an IEEE system and trained with Tensorflow libraries using Keras. | [128] |
| Sliding mode controller (SMC) methodology based on Adaptive Dynamic Programming (ADP) | False data injection attacks | A decentralized control approach to large-scale system security was developed to mitigate the effects of unknown injection attacks. | Decentralized Optimal Control Problem | The test was performed on a two-machine Energy system subjected to 3 separate attacks. | [129] |
| Designs a finite time interval sliding mode controller for Markovian hopping systems | Random injection attacks | A control approach that supports probabilistic injection of false data. | Markovian jump cyber–physical systems | The test was performed with single-link robot arm model. | [130] |
| Observer-based controller | DoS attacks | Proposes a control algorithm approach that is not vulnerable to DoS attacks. | A class of two-timescale cyber–physical systems | The effectiveness of the proposed approach was tested in two types: Comparison Simulation and through the inverted pendulum system controlled by a DC motor. | [131] |
| H∞ controller | DoS attacks | Performs a design study of the H∞ controller to mitigate the effects of the DoS attack. | ICPSs | To demonstrate the effectiveness of the proposed approach, numerical simulations are performed. | [132] |

**Table 3.** *Cont.*

| Method | Attack Point | Purpose | Field of Application | Simulation | Reference |
|---|---|---|---|---|---|
| Resilient control by dynamic nonlinear encoding/decoding and chaotic oscillators. | Malicious attacks, stealthy system integrity attacks, and eavesdropping | It develops a control framework with devices for encoding and decoding disordered signals that can identify stealthy attacks on the cyber–physical system. | ICPSs | For testing and validation of the proposed approach, simulations are performed for the quadruple-tank process. | [133] |
| Offense–defense game model | Malware attacks | Presents an online technique based on the offense-defense game model capable of identifying these malware attacks. | Electrical vehicles | Numerical and dynamic simulation in GAMS and MATLAB software. | [134] |

The power system is considered a critical infrastructure in the control system of a CPS due to the automation of generation, transmission, and distribution operations. In this context, frequency control is a target of these cyberattacks, and Reference [125] sought to tackle this problem by proposing distributed frequency controls based on Model Predictive Control (MPC) to improve the dynamic response of the system and mitigate eventual failures. This controller was tested on an IEEE benchmark system, and through device speed measurement and indirect estimation of the reference value, the controller presents the ability to withstand cyberattacks of denial of service and fake data injection types.

To analyze power system stability control and cybersecurity, Reference [126] presents a real-time test bench for CPS. In this simulator, it is possible for the user to simulate fault situations and analyze the impacts generated. In addition, it presents an adaptive control for a multi-machine power system.

False data injection attacks aim to compromise the satisfactory operation and control system of a CPS by inserting false information into the measurements of sensors and control signals. To mitigate this type of attack, Reference [127] proposes a controller designed from the perspective of power conversion that changes its parameters dynamically as the system suffers cyberattacks. By adjusting the amount of damping insertion, the controller stabilizes and ensures the dynamic operation of the system [127].

Real-time and accurate identification of the location of the attack is important to ensure the smooth operation of the system. Thus, the authors of [128] developed a multivariate methodology capable of accurately detecting false data injection into the CPS in real-time. The proposal consists of a parallel framework that relates Long Short-Term Memory (LSTM) with Temporal Convolutional Neural Network (TCN) [128].

For large systems, Reference [129] presents a decentralized control approach that uses the sliding mode controller (SMC) methodology based on Adaptive Dynamic Programming (ADP) to mitigate the effects of unknown injection attacks. This control strategy was tested by three distinct attacks for a system with two machines [129]. Furthermore, the insertion of false data into the control signal can happen randomly to cause uncertainty and disturbances in the process. Given this vulnerability, the authors of [130] designed a finite time interval sliding mode controller for Markovian hopping systems that supports probabilistic fake data injection.

The application of network technologies in communication and control makes the CPS vulnerable to DoS attacks. Therefore, to combat this type of two-timescale attack, Reference [131] proposes a control algorithm approach using the observer concept for a category of two-timescale CPSs (TTSCPSs) [131]. For an ICPS with a Hybrid Trigger

Mechanism (HTM) subjected to DoS attack, the authors of [132] performed an H∞ controller design study to mitigate the effects of this attack.

There are attacks that target manipulating the process plant conditions to harm the integrity of the system. In this perspective, Reference [133] created a control structure with disorderly signal encoding and decoding devices that can identify stealthy attacks on the CPS. Therefore, it maintains the nominal operating performance without attacks on the system and provides a robust and resilient CPS to attacks.

EVs are also a target for cyberattacks because of their interconnected network of wireless sensors. Reference [134] presents a methodology based on the offense–defense game model capable of identifying these malware attacks and, consequently, preventing them from reaching EVs.

In Table 3, all the discussions mentioned above and research on cyberattacks on control systems are analyzed and detailed.

Thus, the works discussed in this section present defense strategies for protection against cyberattacks such as false data injection, denial of service, random injection, malwares, and eavesdropping on control systems. The defense strategies are based on the development of observer and H∞ based controllers; robust, adaptive, predictive, nonlinear control techniques; game theory; and dynamic programming. Therefore, these are important methodologies found in the literature that seek to improve reliability, resilience, and cybersecurity in the control system of industries, electric transportation, smart grids, and the power system in general.

### *4.3. Cybersecurity in Protection Systems*

The modern power system has increasingly used situation awareness, electronics, and computer technologies in its operation, planning, control, and protection. Consequently, while meaningfully improving multiple processes, it has also become particularly fragile to cyberattacks. Among these vulnerabilities, it is worth noting that attacks on fault relays and other safety devices that compose the protection system in power systems are critical events that can cause blackouts and other major disruptions to the operation of the system. Thus, due to the possibility of network connected operation, in the islanded mode, or new connections of islanded networks, it becomes the protection system one of the main points of interest to ensure cybersecurity in MG. In this category, 10 key works were selected and are shown in Table 4.

**Table 4.** Cybersecurity applications: protection systems [135–144].

| Method | Attack Point | Purpose | Field of Application | Simulation | Reference |
|---|---|---|---|---|---|
| Based on the differences between the calculated and measured overlapping voltages for LCDRs | Injection of false data into LCDRs | The proposed methodology aims to detect the types of injections of false data against LCDRs. | LCDRs | The developed methodology is validated using the IEEE-39 bus model and the OPAL simulator. | [135] |
| A state observer with unknown input | Injection of false data into LCDRs | Detect injection of false data and distinguish it from internal LCDRs operational failures. | LCDRs | The developed methodology is validated using the IEEE-39 bus model. | [136] |
| The developed method consists of passive oscillator circuits | Injection of false data into LCDRs | Presents a study on the impacts of attacks on time synchronization and false data in microgrids and acts to solve the problem from the physical perspective. | LCDRs | The proposed method is analyzed in simulation and validated through numerical analysis. | [137] |
| Model-based on intelligent learning with Multilayer Perceptron | Injection of false data into LCDRs | The detection of cyberattacks against LCDRs is performed using a learning-based framework. | LCDRs | The developed methodology is confirmed using the IEEE-39 bus model. | [138] |

**Table 4.** *Cont.*

| Method | Attack Point | Purpose | Field of Application | Simulation | Reference |
|---|---|---|---|---|---|
| The anomaly-based framework that employs the Isolation Forest algorithm | Injection of false data into LCDRs | Detect cyberattacks and differentiate from a fake attack on systems that use LCDRs as protection. | LCDRs | The developed methodology is validated in benchmark IEEE 9-bus in PSCAD/EMTDC environment. | [139] |
| Methodology based on game theory | Cyberattack on relay configuration in power distribution systems | Ability to detect the best defense plan and mitigate the damage to the protection relays. | Power distribution system | The developed methodology is tested on the IEEE 123-node test feeder. | [140] |
| Multi-Agent Distributed Deep Learning | Injection of false data to the relays | This technique can detect the injection of false data to the relays before it simulates a false fault. | The protection system of a power grid. | The proposed cyberattack detection method is tested on the electrical networks: IEEE 6-bus, IEEE 14-bus, and IEEE 118-bus. | [141] |
| Adaptive technique | Injection of false data to the relays | This methodology has the objective of mitigating false attacks on the protection relays and avoiding power interruptions in the grid. | Protection relays | A real-time digital simulator was used to validate the proposed approach. | [142] |
| Rule-based algorithm and the principle of relay coordination | Malicious attacks on the protection relays | It presents a defense strategy against malicious attacks and unwanted modifications to the protection relays. | Protection relays | The proposed technique is tested and validated on a framework with relays and a real-time digital simulator for cyber–physical systems. | [143] |
| Recurrent neural network with LSTM cells | Cyberattacks and protection system anomalies | Intelligent algorithm with the ability to monitor and detect in real time the anomalies of the protection system caused by malicious attacks. | Transmission protection systems | The proposal is validated on the IEEE test system with relays. | [144] |

Line current differential relays can detect faults accurately and were quickly and have been increasingly used in power system protection. Thus, with the integration of technology with the cyber–physical system, the study of the vulnerabilities of relays to cyberattacks has aroused interest. Thus, Reference [135] investigated the impacts and proposes a methodology based on the differential between measured and calculated voltages for detecting the injection of false data into line current differential relays (LCDRs). The developed methodology was validated using the IEEE-39 bus model and the OPAL simulator. For this problem, the author of [136] proposes a technique based on a state observer with unknown input that can detect the injection of false data and distinguish it from internal operational faults. To make systems using LCDRs more resilient, Reference [137] presents a study on the impacts of attacks on time synchronization and false data in microgrids. The technique proposed in [137] solves the problem from the physical perspective, using a passive oscillator circuit that, under failure, generates as a response a specific damped frequency. In contrast, Reference [138], to solve the problem presented in [137], used artificial intelligence concepts. Thus, the author proposes a model based on intelligent learning with Multilayer Perceptron (MLP) topology [138]. Moreover, for systems that use LCDRs as protection, the author of [139] proposes an anomaly-based framework that employs the

Isolation Forest algorithm to detect cyberattacks and differentiate them from false attacks. This methodology was developed using the IEEE-9 bus model.

The power distribution system also presents vulnerabilities to cyberattacks. Therefore, it is important to improve cybersecurity in these systems. In this perspective, Reference [140] presents a methodology based on game theory that is capable of detecting the best defense plan and mitigating the damage caused to the protection relays in the system.

The protection system of a power grid uses remote relays as defense devices. However, these components are considered critical and present vulnerabilities to cyberattacks. Thus, Reference [141] proposes a robust neural-network-based methodology called Multi-Agent Distributed Deep Learning (MADDL). This technique can detect the injection of false data to the relays before the data simulate a false fault. Reference [142] proposes an adaptive technique in which relays communicate with each other to check the state of the variables at each point of the protection system of a microgrid. This methodology has the objective of mitigating false attacks on the protection relays and avoiding power interruptions in the grid caused by the attack of a false data injection. Reference [143] presents a cooperative defense strategy against unwanted modifications of protective relay settings caused by malicious attacks. The proposed algorithm is based on principles that aim to manage relays.

The transmission system is sensitive to cyberattacks due to embedded electronics and computing technologies in the protection system. From this perspective, Reference [144] developed an intelligent algorithm that was validated in the IEEE test system with relays, which can monitor and detect in real-time possible malicious attacks that cause anomalies to the protection system.

In Table 4, all the discussions mentioned above and research on cyberattacks in protection systems are analyzed and detailed.

Thus, the works discussed in this section present strategies to improve and ensure cybersecurity in the protection system and the defense devices of microgrids. The defense strategies presented are based on AI and deep-learning algorithms, adaptive techniques, passive oscillator circuits, game theory methodology, and state observer control. Therefore, these are important techniques found in the literature that seek to mitigate cyberattacks to improve the reliability, resilience, and cybersecurity of an MG protection system.

### *4.4. Defense Strategies and Future Trends for Cybersecurity*

As discussed in this paper, the current power system is vulnerable and the target of numerous and constant cyberattacks that aim to undermine the planning, operation, maintenance, and supply of power to users. Thus, Sections 4.1–4.3 discussed works on cybersecurity in the areas of monitoring [115–124], control [125–134], and protection [135–144] of cyber–physical systems. The most common types of attacks were cyberattacks of fake data injection, malware attacks, DoS attacks, and eavesdropping. Thus, it is worth noting that the main defense strategies to enhance cybersecurity presented in these research studies focus on protecting and identifying these cyberattacks:

- Strategies based on protection against cyberattacks are related to meters, sensors, aggregators, actuators, defense devices, and all other components that make up the physical part of a MG and a CPS.
- Identification-based strategies aim to mitigate or eliminate the unwanted effects of cyberattacks. Detection can happen in a static manner, in which it seeks to achieve stationary stability, and in a dynamic manner, in which dynamic information is used in the detection process [47].

The defense strategies used in the works discussed in Sections 4.1–4.3 are based on traditional theories and concepts of modern, robust, adaptive, and predictive control: AI, machine-learning, and deep-learning algorithms. However, to improve cybersecurity in an SG, the author [69,145] points out new avenues of research that use digital signal processing techniques; blockchain techniques for SG (Reference [122] used blockchain technology to defend the Reactor Protection System of a nuclear power plant); and use of new techniques for creating cryptography based on quantum computing and, consequently, big data anal-

ysis for making more efficient and reliable cybersecurity algorithms. Creating, updating, developing, and discussing new standards, protocols, and regulations are important defense strategies to improve cybersecurity in MG. Section 5 presents cybersecurity standards and regulations in SGs.

Therefore, based on the current scenario in the power sector, it is possible to infer the following future trends of cyberattacks in MG:

- Modernization of the electricity system: The gradual replacement of conventional power generation by clean energy increases the penetration of renewables, modifies the behavior, and adds the characteristic of intermittent generation to the system. Moreover, the use of new IoT technologies and the integration between devices and sectors provide the emergence of smart grids, which, due to the dependence on the Internet for operation and communication, present cyber vulnerabilities. Thus, the MG needs reliable and resilient cybersecurity in order not to harm its communication, state estimation, frequency control, voltage regulation, and the performance of its applications, such as the possibility of operation in the islanded mode and the connection of other islanded grids.
- Transportation and electrification: The process of electrification of transportation is a strategy that encourages the development, production, and use of electrically powered buses, vehicles, trains, and subways, as well as being an important factor in decreasing the emission of polluting gases into the atmosphere. These technological vehicles connected to charging stations modify and are part of the MG. Thus, this new means of transportation becomes a target of cyberattacks, and the security of charging stations is considered a point of vulnerability and of research interest [146]. From this perspective, the author of [147] designed simulation software to evaluate the cyber vulnerability of electric vehicle charging structures and devices. Therefore, cybersecurity in transportation electrification is a current problem that is under research and development.

## 5. Regulations and Standards

In recent years, the inclusion of new information technologies in the modern power system infrastructure has led it to approach the characteristics of a cyber–physical system. In this way, it presents the benefits, pitfalls, and vulnerabilities of a CPS. Therefore, governments, companies, and technical and scientific organizations continuously seek to create a comprehensive document containing aspects and specifications that regulate and, consequently, increase the safety, reliability, and operation. These documents are referred to as cybersecurity standards and regulations. In this section, some of the key cybersecurity standards and regulations related to smart grids are described.

i. AMI-SER

The advanced metering infrastructure (AMI) of a smart grid has vulnerabilities in its communication infrastructure and in its supporting information infrastructure and, consequently, compromises the cybersecurity of the electric grid [92]. Seeking to address this perspective, the AMI System Security Requirements (AMI-SER) cybersecurity protocol was created. The security guidelines in this document were developed in 2008 by the UCA International users' group (UCAIug) [47,92,148,149]. This protocol specifically addresses cybersecurity requirements for procurement and has geographic coverage in the US. It outlines technical standards to ensure robust security for the advanced metering infrastructure of a smart grid [92]. Thus, this protocol aims to provide a set of requirements that ensure proper operation, adequate availability of services, and reliability and security of the information in the system. AMI is the main component of a smart grid to which this protocol is applied. In addition, this standard presents safety requirements and objectives that can be used in manufacturers' industrial compliance testing [92,148,149]. More details about the standard can be found in [149].

ii. IEC 62351

The IEC 62351 protocol is an international industry standard developed by the International Electrotechnical Commission (IEC) whose first parts were published in 2007 and are constantly being updated [148]. IEC 62351 consists of cybersecurity standards that aim to improve security in smart power system devices and preserve the confidentiality, authenticity, and integrity of information [150]. This standard specifically addresses the cybersecurity of protocols and can be applied to all components of a smart grid architecture [92,148]. In addition, this standard has a global scope and presents technical solutions, safety requirements, and objectives that can be used in industrial compliance testing. The IEC 62351 standard is separated into 16 chapters (IEC 62351-1 through IEC 62351-13; IEC 62351-90-1, IEC 62351-90-2, and IEC 62351-100-1), and each part addresses a distinct area [47,92].

iii. NERC-CIP

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standard establishes minimum parameters to be followed to ensure bulk power system cybersecurity [92,151]. NERC-CIP presents a set of standards and requirements that aim to build a robust and secure framework that is capable of protecting the critical infrastructure and cyber devices of a smart grid and, consequently, assist in its reliable operation [92,148,152]. This standard was published in 2013 with US coverage and presents more general high-level guidance [92]. The NERC-CIP protocol is a standard capable of protecting an enterprise's critical infrastructure and can be applied to address critical system issues such as security management control; identify network hot spots; provide recovery, reporting, and response patterns; address physical and personal security; and standardize boundary regions that present satisfactory electronic security [92,148,152].

iv. NIST Standard

The development of cybersecurity standards and techniques for US smart grids is the responsibility of the National Institute of Standards and Technology (NIST). Thus, in 2010, the NIST standard was published that addresses cyber and information security and risk management [92]. Although it is a protocol created in the US, it is used worldwide in developing companies and systems [92]. This protocol presents high-level technical solutions and general guidelines [92]. References [92,148] present other variations of the NIST standard.

v. NIST SP 800-82

The National Institute of Standards and Technology Special Publication (SP) 800-82 (NIST SP-800-82) is the main NIST guideline governing industrial control and automation system security in the US and is also used worldwide [148]. This protocol, which was published in 2013, presents technical solutions and special suggestions regarding susceptibility and penetration-checking devices [92,148]. In addition, compliance with the standard ensures that the system security control will operate correctly and obtain satisfactory results [47]. The standard can be used in control and automation systems that use the system SCADA [92,148].

vi. NISTIR 7628

Created in 2014 in the US and with global reach, the National Institute of Standards and Technology Interagency Report 7628 (NISTIR 7628) is a guideline for smart grid cybersecurity [148]. For smart system grids, this guide disseminates a set of cybersecurity defense techniques and rules [47,148]. Furthermore, this guide contains 10 chapters and 10 Appendices divided into 3 volumes [47,153], and it is applied to all devices that constitute the smart grid. The full standard can be found in [153].

vii. IEEE 2030 Std.2

Published in 2015 and with worldwide reach, the IEEE 2030 Std.2 standard entitled "IEEE Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure" is a set of standards created by IEEE [153]. This technical guideline

presents 10 chapters and 5 appendices and is responsible for the minimum requirements of Energy storage systems' interoperability [148]. The guideline presents technical solutions with important guidelines, strategies, and definitions that are associated with the current cybersecurity requirements for industrial applications and projects related to an energy storage system in smart grids [148,153]. The full standard can be found in [154].

viii. IEEE C37.240

The use of new intelligent and information technologies in the communication, control, automation, and protection system of power system substations raises concerns from the point of view of cybersecurity. In this context, in 2014, the IEEE published a standard with global scope entitled "IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems" [155]. The standard presents sound technical solutions and engineering practices and is also responsible for providing minimum requirements for the substation communication system to achieve adequate cybersecurity [148,155]. In this way, the standard aims to seek a balance between technical and economic feasibility with current cybersecurity concepts [148,155].

The interested reader is referred to [92,148] for additional works on the smart grid's cybersecurity standards and regulations.

## 6. Conclusions

This paper provides a review of the literature on cybersecurity in cyber–physical systems. The research was motivated by the recent modernization actions and policies in the energy sector, including incentives for the insertion of renewable energy sources, new information technologies, communication, monitoring, and networks allied to IoT concepts, artificial intelligence, machine learning, and modern control techniques. Thus, the current energy system presents the benefits that new technologies have provided, as well as the vulnerabilities and evils associated with modern cyber–physical systems.

The cyber–physical system can be typically described based on a three-layer architecture: perception layer, transport layer, and application layer. In addition, physical components, sensing components, and control and communication components are the three groups of devices that constitute a typical CPS. Power generators, transformers, transmission lines, circuit breakers, switchgear, and power system loads are part of the physical components of a power system. Sensors, actuators, and aggregators are part of the sensing component group. Finally, PLC, DCS, RTU, SCADA, and PMU are part of the control and communication components. To understand and identify vulnerabilities, it is important to understand the interrelationship between the components and layers of a CPS.

Based on the research conducted, it is possible to conclude that cyberattacks are a challenging and critical reality of modern cyber–physical systems. Given the long-term history of attacks and recent major disruptive attacks such as Ukraine's power sector outage in 2015, it is necessary to develop and ensure that adequate protection layers are available and in place at all system levels. Furthermore, it is important to know the classification of the various types of cyberattacks found in the literature to find out and understand how each attack works. Subsequently, planning and creating mechanisms to mitigate and nullify the effects of cyberattacks is necessary. In this context, international technical and scientific institutions such as IEEE, IEC, NIST, and UCAIug, among others, have created a series of standards and regulations to improve cybersecurity in smart grids and the industrial sector. For future works, one must perform a literature survey on the relationship between cyberattacks and cyber terrorism in cyber–physical systems.

**Author Contributions:** L.F.R.M., Y.R.R. and A.C.Z.d.S. worked on the review process and construction of the paper. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** Does not apply.

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

## Abbreviations

| | |
|---|---|
| ACK | acknowledgment |
| ADS | Anomaly Detection System |
| ADP | Adaptive Dynamic Programming |
| AEs | autoencoders |
| AHP | Analytic Hierarchy Process |
| AI | artificial intelligence |
| AMI | advanced metering infrastructure |
| AMI-SER | Advanced Metering Infrastructure System Security Requirements |
| CI | computational intelligence |
| CIA | code injection attacks |
| COVID-19 | coronavirus disease pandemic |
| CPS | cyber–physical systems |
| CP-SAM | Cyber–Physical Security Assessment Metric |
| CPPS | cyber–physical power system |
| CPU | central processing unit |
| DCS | Distributed Control System |
| DDoS | distributed denial of service |
| DOM | document object model |
| DoS | denial of service |
| EV | electric vehicle |
| FDI | false data injection |
| GPS | Global Position System |
| HMI | Human–Machine Interface |
| HTM | Hybrid Trigger Mechanism |
| HTTP | Hypertext Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| ICPSs | industrial cyber–physical systems |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IIoT | Industrial Internet of Things |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IR | infrared |
| LCDRs | line current differential relays |
| LOF | Local Outlier Factor |
| LSTM | Long Short-Term Memory |
| MADDL | Multi-Agent Distributed Deep Learning |
| MCDM | multicriteria decision-making |
| MLP | Multilayer Perceptron |
| ML-RSM | Multilayer Run-Time Security Monitor |
| MG | microgrids |
| MPC | Model Predictive Control |
| NERC-CIP | North American Electric Reliability Corporation Critical Infrastructure Protection |
| NIST | National Institute of Standards and Technology |
| NIST SP | National Institute of Standards and Technology Special Publication |
| NISTIR | National Institute of Standards and Technology Interagency Report |
| NPPs | nuclear power plants |
| OCSVMs | one-class support vector machines |
| PCHD | Port Controlled Hamiltonian with dissipation |
| PLC | Programmable Logic Controller |
| PMU | Phasor Measurement Unit |
| RA | replay attack |

| | |
|---|---|
| RFID | Radio-Frequency Identification |
| RPS | Reactor Protection System |
| RSDBN | regularized sparse deep belief network |
| RTU | Remote Terminal Unit |
| SCADA | Supervisory Control and Data Acquisition |
| SG | smart grid |
| SMC | sliding mode controller |
| SP | Special Publication |
| SYN | synchronization |
| TCN | Temporal Convolutional Neural Network |
| TCP | Transmission Control Protocol |
| TOPSIS | Technique for Order of Preference by Similarity to Ideal Solution |
| TTSCPSs | two-timescale CPSs |
| UCAIug | UCA International users' group |
| UDP | user datagram protocol |

## References


1. De Vries, J. The Industrial Revolution and the Industrious Revolution. *J. Econ. Hist.* **1994**, *54*, 249–270. [CrossRef]
2. Hudson, P. *The Industrial Revolution*, 1st ed.; Bloomsbury Publishing: London, UK, 2014; p. 256. ISBN 9781474225489.
3. Xu, M.; David, J.M.; Kim, S.H. The Fourth Industrial Revolution: Opportunities and Challenges. *Int. J. Financ. Res.* **2018**, *9*, 90–95. [CrossRef]
4. Rohde, R.; Muller, R.M.; Jacobsen, R.; Muller, E.; Perlmutter, S.; Rosenfeld, A.; Wurtele, J.; Groom, D.; Wickham, C. A new estimate of the average Earth surface land temperature spanning 1753 to 2011. *Geoinfor. Geostat. Overv.* **2013**, *1*, 1. [CrossRef]
5. Hansen, J.; Sato, M. Global temperature change. *Proc. Natl. Acad. Sci. USA* **2006**, *103*, 14288–14293. [CrossRef] [PubMed]
6. Nita, I.A.; Sfîcă, L.; Voiculescu, M.; Birsan, M.V.; Micheu, M.M. Changes in the global mean air temperature over land since 1980. *Atmos. Res.* **2022**, *279*, 106392. [CrossRef]
7. Pileggi, S.F.; Lamia, S.A. Climate Change TimeLine: An Ontology to Tell the Story so Far. *IEEE Access* **2020**, *8*, 65294–65312. [CrossRef]
8. Anderson, T.R.; Hawkins, E.D.; Jones, P.J. $CO_2$, the greenhouse effect and global warming: From the pioneering work of Arrhenius and Callendar to today's Earth System Models. *Endeavour* **2016**, *50*, 178–187. [CrossRef]
9. Rachel, W. Chapter 11: Impacts of global climate change at different annual mean global temperature increases. In *Avoiding Dangerous Climate Change*, 1st ed.; Schellnhuber, H.M., Cramer, W., Nakicenovic, N., Wigley, T., Yohe, G., Eds.; Cambridge University Press: Cambridge, UK, 2006; pp. 93–94. ISBN 9780521864718.
10. Arnell, N.W. The implications of climate change for emergency planning. *Int. J. Disaster Risk Reduct.* **2022**, *83*, 103425. [CrossRef]
11. Hallegatte, S.; Rozenberg, J. Climate change through a poverty lens. *Nat. Clim Chang.* **2017**, *7*, 250–256. [CrossRef]
12. Diffenbaugh, N.S.; Burke, M. Global warming has increased global economic inequality. *Proc. Natl. Acad. Sci. USA* **2019**, *116*, 9808–9813. [CrossRef]
13. Raymakers, A.J.N.; Sue-Chue-Lam, C.; Haldane, V.; Cooper-Reed, A.; Toccalino, D. Climate change, sustainability, and health services research. *Health Policy Technol.* **2022**, *12*, 100694. [CrossRef]
14. Ahmadian, E.; Sodagar, B.; Bingham, C.; Elnokaly, A.; Mills, G. Effect of urban built form and density on building energy performance in temperate climates. *Energy Build.* **2021**, *236*, 110762. [CrossRef]
15. Ahmadian, E.; Bingham, C.; Elnokaly, A.; Sodagar, B.; Verhaert, I. Impact of Climate Change and Technological Innovation on the Energy Performance and Built form of Future Cities. *Energies* **2022**, *15*, 8592. [CrossRef]
16. Ahmadian, E.; Byrd, H.; Sodagar, B.; Matthewman, S.; Kenney, C.; Mills, G. Energy and the form of cities: The counterintuitive impact of disruptive technologies. *Archit. Sci. Rev.* **2019**, *62*, 145–151. [CrossRef]
17. Arnold, G.W. Challenges and opportunities in smart grid: A position article. *Proc. IEEE* **2011**, *99*, 922–927. [CrossRef]
18. Davies, S. Grid gets the smarts [power smart grid]. *Eng. Technol.* **2013**, *7*, 42–45. [CrossRef]
19. Gómez-Expósito, A.; Arcos-Vargas, A.; Maza-Ortega, J.M.; Rosendo-Macias, J.A.; Alvarez-Cordero, G.; Carillo-Aparicio, S.; Gonzalez-Lara, J.; Morales-Wagner, D.; Gonzalez-Garcia, T. City-Friendly Smart Network Technologies and Infrastructures: The Spanish Experience. *Proc. IEEE* **2018**, *106*, 626–660. [CrossRef]
20. Pustokhin, D.A.; Pustokhina, I.V.; Rani, P.; Kansal, V.; Elhoseny, M.; Joshi, G.P.; Shankar, K. Optimal deep learning approaches and healthcare big data analytics for mobile networks toward 5G. *Comput. Electr. Eng.* **2021**, *95*, 107376. [CrossRef]
21. Longo, F.; Padovano, A.; Aiello, G.; Fusto, C.; Certa, A. How 5G-based industrial IoT is transforming human-centered smart factories: A Quality of Experience model for Operator 4.0 applications. *IFAC-PapersOnLine* **2021**, *54*, 255–262. [CrossRef]
22. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]
23. Navarro, E.M.; Alvarez, A.N.R.; Anguiano, F.I. S A new telesurgery generation supported by 5G technology: Benefits and future trends. *Procedia Comput. Sci.* **2022**, *200*, 31–38. [CrossRef]

24. Meshram, D.A.; Patil, D.D. 5G Enabled Tactile Internet for Tele-Robotic Surgery. *Procedia Comput. Sci.* **2020**, *171*, 2618–2625. [CrossRef]
25. Hakak, S.; Gadekallu, T.R.; Maddikunta, P.K.R.; Ramu, S.P.; M, P.; De Alwis, C.; Liyanage, M. Autonomous vehicles in 5G and beyond: A survey. *Veh. Commun.* **2023**, *39*, 100551. [CrossRef]
26. Energy.gov. National Cyber-Informed Engineering Strategy from the U.S. Department of Energy. Available online: https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf (accessed on 10 December 2022).
27. gov.uk. Government Cyber Security Strategy: Building a Cyber Resilient Public Sector. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf (accessed on 10 December 2022).
28. Institute for Security Technology Studies. Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report. 2004. Available online: https://priv.gg/e/ISTSLawEnforcementResearchandDevelopmentAgendaJune2004.pdf (accessed on 10 December 2022).
29. Smith, E.; Corzine, S.; Racey, D.; Dunne, P.; Hassett, C.; Weiss, J. Going beyond cybersecurity compliance: What power and utility companies really need to consider. *IEEE Power Energy Mag.* **2016**, *14*, 48–56. [CrossRef]
30. Liu, C.C.; Bedoya, J.C.; Sahani, N.; Stefanov, A.; Appiah-Kubi, J.; Sun, C.C.; Lee, J.Y.; Zhu, R. Cyber–Physical System Security of Distribution Systems. *Found. Trends®Electr. Energy Syst.* **2021**, *4*, 346–410. [CrossRef]
31. Li, Z.; Shahidehpour, M.; Aminifar, F. Cybersecurity in Distributed Power Systems. *Proc. IEEE* **2017**, *105*, 1367–1388. [CrossRef]
32. Vaidya, T. 2001–2013: Survey and Analysis of Major Cyberattacks. *arXiv* **2015**, arXiv:1507.06673. [CrossRef]
33. Hemsley, K.; Fisher, R. A History of Cyber Incidents and Threats Involving Industrial Control Systems. In *Critical Infrastructure Protection XII, Proceedings of the 12th IFIP WG 11.10 International Conference, ICCIP 2018, Arlington, VA, USA, 12–14 March 2018*; Springer: Berlin/Heidelberg, Germany, 2018; Volume 542. [CrossRef]
34. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications. *IEEE Access* **2020**, *8*, 151019–151064. [CrossRef]
35. Baezner, M.; Robin, P. *Stuxnet*; Center for Security Studies (CSS), ETH Zürich: Zürich, Switzerland, 2017; pp. 1–14. [CrossRef]
36. Saxena, S.; Bhatia, S.; Gupta, R. Cybersecurity Analysis of Load Frequency Control in Power Systems: A Survey. *Designs* **2021**, *5*, 52. [CrossRef]
37. Case. Defense Use. Analysis of the Cyber Attack on the Ukrainian Power Grid. *Electr. Inf. Shar. Anal. Cent. (E-ISAC)* **2016**, *388*, 1–29. Available online: https://africautc.org/wp-content/uploads/2018/05/E-ISAC_SANS_Ukraine_DUC_5.pdf (accessed on 10 December 2022).
38. Musleh, A.S.; Chen, G.; Dong, Z.Y. A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2019**, *11*, 2218–2234. [CrossRef]
39. Muthuppalaniappan, M.; Stevenson, K. Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *Int. J. Qual. Health Care* **2021**, *33*, mzaa117. [CrossRef] [PubMed]
40. Venkatachary, S.K.; Prasad, J.; Samikannu, R. Cybersecurity and cyber terrorism-in energy sector–a review. *J. Cyber Secur. Technol.* **2018**, *2*, 111–130. [CrossRef]
41. Pate, A. Terrorism Trends with a Focus on Energy and Mining. *START Res. Brief* **2015**, 1–2. Available online: https://www.start.umd.edu/pubs/START_TerrorismEnergyAttacks_ResearchBrief_June2015.pdf (accessed on 10 December 2022).
42. Karamdel, S.; Liang, X.; Faried, S.O.; Mitolo, M. Optimization Models in Cyber-Physical Power Systems: A Review. *IEEE Access* **2022**, *10*, 130469–130486. [CrossRef]
43. He, S.; Zhou, Y.; Lv, X.; Chen, W. Detection Method for Tolerable False Data Injection Attack Based on Deep Learning Framework. In Proceedings of the Chinese Automation Congress (CAC), Shanghai, China, 6–8 November 2020; pp. 6717–6721. [CrossRef]
44. Du, D.; Zhu, M.; Li, X.; Fei, M.; Bu, S.; Wu, L.; Li, K. A Review on Cybersecurity Analysis, Attack Detection, and Attack Defense Methods in Cyber-Physical Power Systems. *J. Mod. Power Syst. Clean Energy* **2023**, *11*, 727–743. [CrossRef]
45. Duo, W.; Zhou, M.; Abusorrah, A. A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 784–800. [CrossRef]
46. Surya, S.; Srinivasan, M.K.; Williamson, S. Technological Perspective of Cyber Secure Smart Inverters Used in Power Distribution System: State of the Art Review. *Appl. Sci.* **2021**, *11*, 8780. [CrossRef]
47. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27. [CrossRef]
48. Deng, R.; Xiao, G.; Lu, R.; Liang, H.; Vasilakos, A.V. False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey. *IEEE Trans. Ind. Inf.* **2017**, *13*, 411–423. [CrossRef]
49. Wang, Q.; Tai, W.; Tang, Y.; Ni, M. Review of the false data injection attack against the cyber-physical power system. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 101–107. [CrossRef]
50. Brar, H.S.; Kumar, G. Cybercrimes: A Proposed Taxonomy and Challenges. *J. Comput. Netw. Commun.* **2018**, *2018*, 1798659. [CrossRef]
51. Alsuwian, T.; Shahid Butt, A.; Amin, A.A. Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review. *Sustainability* **2022**, *14*, 14226. [CrossRef]

52. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* **2014**, *1*, 53–66. [CrossRef]
53. Biju, J.M.; Gopal, N.; Prakash, A.J. Cyber attacks and its different types. *Int. Res. J. Eng. Technol.* **2019**, *6*, 4849–4852.
54. Neira, A.B.; Kantarci, B.; Nogueira, M. Distributed denial of service attack prediction: Challenges, open issues and opportunities. *Comput. Netw.* **2023**, *222*, 109553. [CrossRef]
55. Osanaiye, O.; Choo, K.K.R.; Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *J. Netw. Comput. Appl.* **2016**, *67*, 147–165. [CrossRef]
56. Kishore, P.K.; Ramamoorthy, S.; Rajavarman, V.N. ARTP: Anomaly based real time prevention of Distributed Denial of Service attacks on the web using machine learning approach. *Int. J. Intell. Netw.* **2023**, *4*, 38–45. [CrossRef]
57. Hoque, N.; Bhattacharyya, D.K.; Kalita, J.K. Botnet in DDoS Attacks: Trends and Challenges. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2242–2270. [CrossRef]
58. Kaushik, A.K.; Joshi, R.C. Network forensic system for ICMP attacks. *Int. J. Comput. Appl.* **2010**, *2*, 14–21. [CrossRef]
59. Jaafar, G.A.; Abdullah, S.M.; Ismail, S. Review of Recent Detection Methods for HTTP DDoS Attack. *J. Comput. Netw. Commun.* **2019**, *2019*, 1283472. [CrossRef]
60. Comer, D. *Computer Networks and Internets with Internet Applications*, 4th ed.; Pearson Education: Noida, India, 2004; pp. 1–719. ISBN 817758927X.
61. Mahjabin, T.; Xiao, Y.; Sun, G.; Jiang, W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1–33. [CrossRef]
62. Salim, M.M.; Rathore, S.; Park, J.H. Distributed denial of service attacks and its defenses in IoT: A survey. *J. Supercomput.* **2020**, *76*, 5320–5363. [CrossRef]
63. Alnabulsi, H.; Islam, R.; Talukder, M. GMSA: Gathering Multiple Signatures Approach to Defend Against Code Injection Attacks. *IEEE Access* **2018**, *6*, 77829–77840. [CrossRef]
64. Shar, L.K.; Tan, H.B.K. Defending against Cross-Site Scripting Attacks. *Computer* **2012**, *45*, 55–62. [CrossRef]
65. Yusof, I.; Pathan, A.S.K. Mitigating Cross-Site Scripting Attacks with a Content Security Policy. *Computer* **2016**, *49*, 56–63. [CrossRef]
66. Cohen, F. Information system attacks: A preliminary classification scheme. *Comput. Secur.* **1997**, *16*, 29–46. [CrossRef]
67. Ahmad, D.R.M.; Dubrawsky, I.; Flynn, H.; Grand, J.K.; Graham, R.; Johnson, N.L.; Kaminsky, D.E.; Lynch, F.W.; Manzuik, S.W.; Permeh, R.; et al. (Eds.) *Chapter 11—Session Hijacking. Hack Proofing Your Network*, 2nd ed.; Syngress: Rockland, MA, USA, 2002; pp. 407–441. [CrossRef]
68. Li, Q.; Wang, F.; Wang, J.; Li, W. LSTM-Based SQL Injection Detection Method for Intelligent Transportation System. *IEEE Trans. Veh. Technol.* **2019**, *68*, 4182–4191. [CrossRef]
69. Ghiasi, M.; Niknam, T.; Wang, Z.; Mehrandezh, M.; Dehghani, M.; Ghadimi, N. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electr. Power Syst. Res.* **2023**, *215*, 108975. [CrossRef]
70. Mokhtar, B.; Azab, M. Survey on Security Issues in Vehicular Ad Hoc Networks. *Alex. Eng. J.* **2015**, *54*, 1115–1126. [CrossRef]
71. Ortolani, S.; Giuffrida, C.; Crispo, B. Unprivileged Black-Box Detection of User-Space Keyloggers. *IEEE Trans. Dependable Secur. Comput.* **2013**, *10*, 40–52. [CrossRef]
72. Bhardwaj, A.; Goundar, S. Keyloggers: Silent cyber security weapons. *Netw. Secur.* **2020**, *2020*, 14–19. [CrossRef]
73. Sreenivas, R.S.; Anitha, R. Detecting keyloggers based on traffic analysis with periodic behaviour. *Netw. Secur.* **2011**, *2011*, 14–19. [CrossRef]
74. Sun, H.M.; Chen, Y.H.; Lin, Y.H. oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks. *IEEE Trans. Inf. Forensics Secur.* **2011**, *7*, 651–663. [CrossRef]
75. Song, J.; Wang, D.; Yun, Z.; Han, X. Alphapwd: A Password Generation Strategy Based on Mnemonic Shape. *IEEE Access* **2019**, *7*, 119052–119059. [CrossRef]
76. Yu, X.; Wang, Z.; Li, Y.; Li, L.; Zhu, W.T.; Song, L. EvoPass: Evolvable graphical password against shoulder-surfing attacks. *Comput. Secur.* **2017**, *70*, 179–198. [CrossRef]
77. Ye, B.; Guo, Y.; Zhang, L.; Guo, X. An empirical study of mnemonic password creation tips. *Comput. Secur.* **2019**, *85*, 41–50. [CrossRef]
78. Abrishamchi, M.A.N.; Zainal, A.; Ghaleb, F.A.; Qasem, S.N.; Albarrak, A.M. Smart Home Privacy Protection Methods against a Passive Wireless Snooping Side-Channel Attack. *Sensors* **2022**, *22*, 8564. [CrossRef] [PubMed]
79. Edwards, M.; Larson, R.; Green, B.; Rashid, A.; Baron, A. Panning for gold: Automatically analysing online social engineering attack surfaces. *Comput. Secur.* **2017**, *69*, 18–34. [CrossRef]
80. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
81. Syafitri, W.; Shukur, Z.; Mokhtar, U.A.; Sulaiman, R.; Ibrahim, M.A. Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access* **2022**, *10*, 39325–39343. [CrossRef]
82. Lee, J.; Bagheri, B.; Kao, H.A. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
83. Baheti, R.; Gill, H. Cyber-physical systems. *Impact Control Technol.* **2011**, *12*, 161–166.

84. Lee, E.A. The Past, Present and Future of Cyber-Physical Systems: A Focus on Models. *Sensors* **2015**, *15*, 4837–4869. [CrossRef] [PubMed]
85. Abdelmalak, M.; Venkataramanan, V.; Macwan, R. A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems. *IEEE Access* **2022**, *10*, 99875–99896. [CrossRef]
86. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* **2020**, *77*, 103201. [CrossRef]
87. Lee, J.; Lapira, E.; Bagheri, B.; Kao, H. Recent advances and trends in predictive manufacturing systems in big data environment. *Manuf. Lett.* **2013**, *1*, 38–41. [CrossRef]
88. Amin, M.; El-Sousy, F.F.M.; Aziz, G.A.A.; Gaber, K.; Mohammed, O.A. CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review. *IEEE Access* **2021**, *9*, 38571–38601. [CrossRef]
89. Chen, H. Applications of cyber-physical system: A literature review. *J. Ind. Integr. Manag.* **2017**, *2*, 1–28. [CrossRef]
90. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97. [CrossRef]
91. Ali, S.; Balushi, T.A.; Nadir, Z.; Hussain, O.K. *Cyber Security for Cyber Physical Systems*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 1–174. [CrossRef]
92. Hasan, M.K.; Habib, A.K.M.A.; Shukur, Z.; Ibrahim, F.; Islam, S.; Razzaque, M.A. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *J. Netw. Comput. Appl.* **2023**, *209*, 103540. [CrossRef]
93. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
94. Mao, X.; Li, X.; Huang, Y.; Shi, J.; Zhang, Y. Programmable Logic Controllers Past Linear Temporal Logic for Monitoring Applications in Industrial Control Systems. *IEEE Trans. Ind. Informat.* **2022**, *18*, 4393–4405. [CrossRef]
95. Alphonsus, E.R.; Abdullah, M.O. A review on the applications of programmable logic controllers (PLCs). *Renew. Sust. Energy Rev.* **2016**, *60*, 1185–1205. [CrossRef]
96. Tang, W.; Daoutidis, P. Distributed control and optimization of process system networks: A review and perspective. *Chin. J. Chem. Eng.* **2019**, *27*, 1461–1473. [CrossRef]
97. Chen, L.; Tang, J.; Bian, X.; Zhan, S.; Lu, X.; Chang, Y. Condition assessment of distribution automation remote terminal units based on double-layer improved cloud model. *Energy Rep.* **2022**, *8*, 408–425. [CrossRef]
98. Kazemi, A.A.R.; Dehghanian, P. A practical approach on optimal RTU placement in power distribution systems incorporating fuzzy sets theory. *Int. J. Electr. Power Energy Syst.* **2012**, *37*, 31–42. [CrossRef]
99. Shammah, A.A.E.; El-Ela, A.A.; Azmy, A.M. Optimal location of remote terminal units in distribution systems using genetic algorithm. *Electr. Power Syst. Res.* **2012**, *89*, 165–170. [CrossRef]
100. Yadav, G.; Paul, K. Architecture and security of SCADA systems: A review. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100433. [CrossRef]
101. Sheng, C.; Yao, Y.; Fu, Q.; Yang, W. A cyber-physical model for SCADA system and its intrusion detection. *Comput. Netw.* **2021**, *185*, 107677. [CrossRef]
102. Sajid, A.; Abbas, H.; Saleem, K. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access* **2016**, *4*, 1375–1384. [CrossRef]
103. Gumaei, A.; Hassan, M.M.; Huda, S.; Hassan, M.R.; Camacho, D.; Ser, J.D.; Fortino, G. A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids. *Appl. Soft Comput.* **2020**, *96*, 106658. [CrossRef]
104. Vanfretti, L.; Baudette, M.; White, A.D. *Chapter 31—Monitoring and Control of Renewable Energy Sources Using Synchronized Phasor Measurements. Renewable Energy Integration*; Academic Press: Cambridge, MA, USA, 2017; pp. 419–434. [CrossRef]
105. *IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005)*; IEEE Standard for Synchrophasor Measurements for Power Systems. IEEE: Piscataway, NJ, USA, 2011; pp. 1–61. [CrossRef]
106. Kiio, M.N.; Wekesa, C.W.; Kamau, S.I. Evaluating Performance of a Linear Hybrid State Estimator Utilizing Measurements From RTUs and Optimally Placed PMUs. *IEEE Access* **2022**, *10*, 63113–63131. [CrossRef]
107. Azizi, S.; Gharehpetian, G.B.; Dobakhshari, A.S. Optimal Integration of Phasor Measurement Units in Power Systems Considering Conventional Measurements. *IEEE Trans. Smart Grid* **2013**, *4*, 1113–1121. [CrossRef]
108. Gabbar, H.A. Chapter 2—Smart energy grid infrastructures and interconnected micro energy grids. In *Smart Energy Grid Engineering*; Academic Press: Cambridge, MA, USA, 2017; pp. 23–45. [CrossRef]
109. Paul, S.; Ding, F.; Utkarsh, K.; Liu, W.; O'Malley, M.J.; Barnett, J. On Vulnerability and Resilience of Cyber-Physical Power Systems: A Review. *IEEE Syst. J.* **2022**, *16*, 2367–2378. [CrossRef]
110. Davidson, C.; Andel, T.; Yampolskiy, M.; McDonald, T.; Glisson, B.; Thomas, T. On SCADA PLC and fieldbus cyber-security. In Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018, Washington, DC, USA, 8–9 March 2018; pp. 140–148.
111. Ghaleb, A.; Zhioua, S.; Almulhem, A. On PLC network security. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 62–69. [CrossRef]
112. Alsabbagh, W.; Langendörfer, P. A Flashback on Control Logic Injection Attacks against Programmable Logic Controllers. *Automation* **2022**, *3*, 596–621. [CrossRef]

113. Han, S.; Lee, K.; Cho, S.; Park, M. Anomaly Detection Based on Temporal Behavior Monitoring in Programmable Logic Controllers. *Electronics* **2021**, *10*, 1218. [CrossRef]
114. Hajda, J.; Jakuszewski, R.; Ogonowski, S. Security Challenges in Industry 4.0 PLC Systems. *Appl. Sci.* **2021**, *11*, 9785. [CrossRef]
115. Khan, M.T.; Tomić, I. Securing Industrial Cyber–Physical Systems: A Run-Time Multilayer Monitoring. *IEEE Trans. Ind. Inform.* **2021**, *17*, 6251–6259. [CrossRef]
116. Liu, J.; Zhang, W.; Ma, T.; Tang, Z.; Xie, Y.; Gui, W.; Niyoyita, J.P. Toward security monitoring of industrial Cyber-Physical systems via hierarchically distributed intrusion detection. *Expert Syst. Appl.* **2020**, *158*, 113578. [CrossRef]
117. Marino, D.L.; Wickramasinghe, C.S.; Tsouvalas, B.; Rieger, C and M. Manic. Data-Driven Correlation of Cyber and Physical Anomalies for Holistic System Health Monitoring. *IEEE Access* **2021**, *9*, 163138–163150. [CrossRef]
118. Fausto, A.; Gaggero, G.B.; Patrone, F.; Girdinio, P.; Marchese, M. Toward the Integration of Cyber and Physical Security Monitoring Systems for Critical Infrastructures. *Sensors* **2021**, *21*, 6970. [CrossRef] [PubMed]
119. Venkataramanan, V.; Hahn, A.; Srivastava, A. CP-SAM: Cyber-Physical Security Assessment Metric for Monitoring Microgrid Resiliency. *IEEE Trans. Smart Grid* **2020**, *11*, 1055–1065. [CrossRef]
120. Li, Q.; Meng, S.; Zhang, S.; Wu, M.; Zhang, J.; Ahvanooey, M.T.; Aslam, M.S. Safety Risk Monitoring of Cyber-Physical Power Systems Based on Ensemble Learning Algorithm. *IEEE Access* **2019**, *7*, 24788–24805. [CrossRef]
121. Alghassab, M. Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector. *Energies* **2022**, *15*, 218. [CrossRef]
122. Choi, M.K.; Yeun, C.Y.; Seong, P.H. A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology. *IEEE Access* **2020**, *8*, 118732–118740. [CrossRef]
123. Bin Mofidul, R.; Alam, M.M.; Rahman, M.H.; Jang, Y.M. Real-Time Energy Data Acquisition, Anomaly Detection, and Monitoring System: Implementation of a Secured, Robust, and Integrated Global IIoT Infrastructure with Edge and Cloud AI. *Sensors* **2022**, *22*, 8980. [CrossRef]
124. Poltavtseva, M.; Shelupanov, A.; Bragin, D.; Zegzhda, D.; Alexandrova, E. Key Concepts of Systemological Approach to CPS Adaptive Information Security Monitoring. *Symmetry* **2021**, *13*, 2425. [CrossRef]
125. Chen, C.; Zhang, K.; Ni, M.; Wang, Y. Cyber-attack-tolerant Frequency Control of Power Systems. *J. Mod. Power Syst. Clean Energy* **2021**, *9*, 307–315. [CrossRef]
126. Poudel, S.; Ni, Z.; Malla, N. Real-time cyber physical system testbed for power system security and control. *Int. J. Electr. Power Energy Syst.* **2017**, *90*, 124–133. [CrossRef]
127. Zhao, Y.; Chen, Z.; Zhou, C.; Tian, Y.C.; Qin, Y. Passivity-Based Robust Control Against Quantified False Data Injection Attacks in Cyber-Physical Systems. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1440–1450. [CrossRef]
128. Hegazy, H.I.; Tag Eldien, A.S.; Tantawy, M.M.; Fouda, M.M.; TagElDien, H.A. Real-Time Locational Detection of Stealthy False Data Injection Attack in Smart Grid: Using Multivariate-Based Multi-Label Classification Approach. *Energies* **2022**, *15*, 5312. [CrossRef]
129. Song, J.; Huang, L.Y.; Karimi, H.R.; Niu, Y.; Zhou, J. ADP-Based Security Decentralized Sliding Mode Control for Partially Unknown Large-Scale Systems Under Injection Attacks. *IEEE Trans. Circuits Syst. I. Regul. Pap.* **2020**, *67*, 5290–5301. [CrossRef]
130. Cao, Z.; Niu, Y.; Song, J. Finite-Time Sliding-Mode Control of Markovian Jump Cyber-Physical Systems Against Randomly Occurring Injection Attacks. *IEEE Trans. Automat. Contr.* **2020**, *65*, 1264–1271. [CrossRef]
131. Zhang, Y.; Ma, L.; Wang, G.; Yang, C.; Zhou, L.; Dai, W. Observer-Based Control for the Two-Time-Scale Cyber-Physical Systems: The Dual-Scale DoS Attacks Case. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 3369–3379. [CrossRef]
132. Wang, M.; Geng, Y.; Wang, J.; Liu, K.; Che, X.; Wei, Q. H∞ Control for ICPS with Hybrid-Triggered Mechanism Encountering Stealthy DoS Jamming Attacks. *Actuators* **2022**, *11*, 193. [CrossRef]
133. Joo, Y.; Qu, Z.; Namerikawa, T. Resilient Control of Cyber-Physical System Using Nonlinear Encoding Signal Against System Integrity Attacks. *IEEE Trans. Automat. Contr.* **2021**, *66*, 4334–4341. [CrossRef]
134. Alsokhiry, F.; Annuk, A.; Kabanen, T.; Mohamed, M.A. A Malware Attack Enabled an Online Energy Strategy for Dynamic Wireless EVs within Transportation Systems. *Mathematics* **2022**, *10*, 4691. [CrossRef]
135. Ameli, A.; Hooshyar, A.; El-Saadany, E.F. Development of a Cyber-Resilient Line Current Differential Relay. *IEEE Trans. Ind. Informat.* **2019**, *15*, 305–318. [CrossRef]
136. Ameli, A.; Hooshyar, A.; El-Saadany, E.F.; Youssef, A.M. An Intrusion Detection Method for Line Current Differential Relays. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 329–344. [CrossRef]
137. Ameli, A.; Saleh, K.A.; Kirakosyan, A.; El-Saadany, E.F.; Salama, M.M.A. An Intrusion Detection Method for Line Current Differential Relays in Medium-Voltage DC Microgrids. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3580–3594. [CrossRef]
138. Ameli, A.; Ayad, A.; El-Saadany, E.F.; Salama, M.M.A.; Youssef, A.M. A Learning-Based Framework for Detecting Cyber-Attacks Against Line Current Differential Relays. *IEEE Trans. Power Deliv.* **2021**, *36*, 2274–2286. [CrossRef]
139. Saber, A.M.; Youssef, A.; Svetinovic, D.; Zeineldin, H.H.; El-Saadany, E.F. Anomaly-Based Detection of Cyberattacks on Line Current Differential Relays. *IEEE Trans. Smart Grid* **2022**, *13*, 4787–4800. [CrossRef]
140. Ganjkhani, M.; Hosseini, M.M.; Parvania, M. Optimal Defensive Strategy for Power Distribution Systems Against Relay Setting Attacks. *IEEE Trans. Power Deliv.* **2022**, *38*, 1499–1509. [CrossRef]
141. Rajaee, M.; Mazlumi, K. Multi-Agent Distributed Deep Learning Algorithm to Detect Cyber-Attacks in Distance Relays. *IEEE Access* **2023**, *11*, 10842–10849. [CrossRef]

142. Gutierrez-Rojas, D.; Demidov, I.; Kontou, A.; Lagos, D.; Sahoo, S.; Nardelli, P.J. Operational Issues on Adaptive Protection of Microgrids due to Cyber Attacks. *IEEE Trans. Circuits Syst. II Express Briefs* **2023**. [CrossRef]
143. Nuqui, R.; Hong, J.; Kondabathini, A.; Ishchenko, D.; Coats, D. A Collaborative Defense for Securing Protective Relay Settings in Electrical Cyber Physical Systems. In Proceedings of the Resilience Week (RWS), Denver, CO, USA, 20–23 August 2018; pp. 49–54. [CrossRef]
144. Ahmed, A.; Krishnan, V.V.G.; Foroutan, S.A.; Touhiduzzaman, M.; Rublein, C.; Srivastava, A.; Wu, Y.; Hahn, A.; Suresh, S. Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems. *IEEE Trans. Ind. Appl.* **2019**, *55*, 6313–6323. [CrossRef]
145. Kaur, J.; Ramkumar, K.R. The recent trends in cyber security: A review. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 5766–5781. [CrossRef]
146. Feng, H.; Tavakoli, R.; Onar, O.C.; Pantic, Z. Advances in High-Power Wireless Charging Systems: Overview and Design Considerations. *IEEE Trans. Transp. Electrif.* **2020**, *6*, 886–919. [CrossRef]
147. Sanghvi, A.; Markel, T. Cybersecurity for Electric Vehicle Fast-Charging Infrastructure. In Proceedings of the 2021 IEEE Transportation Electrification Conference & Expo (ITEC), Chicago, IL, USA, 21–25 June 2021. [CrossRef]
148. Leszczyna, R. Standards on cyber security assessment of smart grid. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 70–89. [CrossRef]
149. Brown, B.; Singletary, B.; Willke, B.; Bennett, C.; Highfill, D.; Houseman, D.; Cleveland, F.; Lipson, H.; Ivers, J.; Gooding, J.; et al. *AMI System Security Requirements*; v1.01; Technical Report; 2008. Available online: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-AMI_System_Security_Requirements_updated.pdf (accessed on 25 February 2023).
150. Schlegel, R.; Obermeier, S.; Schneider, J. A security evaluation of IEC 62351. *J. Inf. Secur. Appl.* **2017**, *34*, 197–204. [CrossRef]
151. Christensen, D.; Martin, M.; Gantumur, E.; Mendrick, B. Risk Assessment at the Edge: Applying NERC CIP to Aggregated Grid-Edge Resources. *Electr. J.* **2019**, *32*, 50–57. [CrossRef]
152. Parks, R.C.; Rogers, E. Vulnerability Assessment for Critical Infrastructure Control Systems. *IEEE Secur. Priv.* **2008**, *6*, 37–43. [CrossRef]
153. *NISTIR 7628: Guidelines for Smart Grid Cyber Security: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*; The Smart Grid Interoperability Panel–Cyber Security Working Group: Washington, DC, USA, 2010. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2010/NIST.IR.7628.pdf (accessed on 25 February 2023).
154. *IEEE Std 2030.2-2015*; IEEE Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure. IEEE: Piscataway, NJ, USA, 2015; pp. 1–138. [CrossRef]
155. *IEEE Std C37.240-2014*; IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems. IEEE: Piscataway, NJ, USA, 2015; pp. 1–38. [CrossRef]


**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.